

Basic Firewall Configuration

Version 1.2



Agenda

- Platform
- Ways to Manage
- Configuration Management
- Initial Configuration
- Interfaces
- Zones
- DHCP
- NAT
- Objects
- Licenses and Profiles
- Security Policies
- Routing
- Policy Based Forwarding
- USER-ID
- Troubleshooting
- Resources

Platform

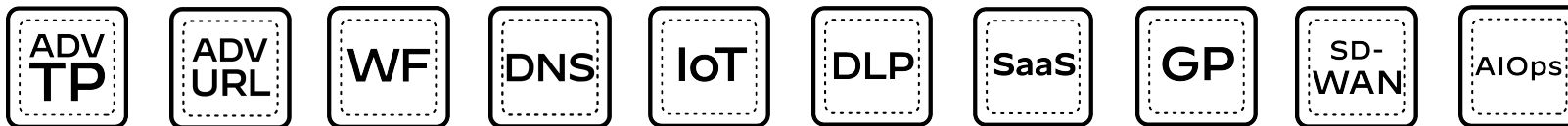
Palo Alto Networks Portfolio coverage

Physical Firewalls		Cloud based Secure access		Detect & Response / XDR				
ML-Powered Next-Generation Firewall		Secure Access Service Edge		Extended Detection and Response				
App-ID User-ID Content-ID Device-ID		FWaaS Secure Web Gateway Zero Trust Network Access		Endpoint Threat Prevention Endpoint Detection & Response Behavioral Analytics Managed Detection & Response				
Virtual Firewalls		Cloud Security		SOC automation / XSOAR				
Virtual Next-Generation Firewall		Cloud Native Security Platform		Extended Security Orchestration, Automation and Response				
App-ID User-ID Content-ID Device-ID		Protection Cloud Network Security Cloud Infrastructure		Security Orchestration, Automation & Response Threat Intelligence Management				
Containerized Firewalls		SD-WAN		Attack Surface Management / Xpanse				
Containerized Next-Generation Firewall		Next-Generation SD-WAN		Attack Surface Management				
App-ID User-ID Content-ID Device-ID		SD-WAN		Internet-Connected Asset Discovery & Mitigation				
Management tool								
Firewall Management								
Unit 42 Security Consulting Services								
Incident Response		Digital Forensics	Proactive Services	Exec & BoD Advisory	Cybersecurity Services			
Ransomware BEC Cloud APT PCI		Forensics Insider Threat Expert Witness	Ransomware BEC Cyber Breach Assessments	vCISO Program Design Strategy Review M&A	Data Breach Response Cyber Risk & Resilience Mgmt Incident Response Services			
Additional Services								
Professional & Support Services								
Resident Engineering Professional Services Focused Services								
Cloud-Delivered Security Services								
DNS Security	Threat Prevention	URL Filtering	WildFire	IoT Security	GlobalProtect	SD-WAN	Data Loss Prevention	Prisma SaaS
DNS Attack Prevention	Exploit, Malware, C2 Prevention	Malicious Site & Phishing Prevention	Malware Prevention	Enterprise IoT Security	Mobile User Security	Secure Branch Connectivity	Data Protection & Compliance	In-line & API SaaS Application Security

Platform Components

Panorama or Strata Cloud Manager

Security Subscriptions



APP-ID



Content-ID



Device-ID

PAN-OS



User-ID



Cloud Identity



Decryption

**Hardware
PA-Series**

**Software
VM-Series / CN-Series**

**Cloud Service
Prisma Access**

Hardware: PA-Series

World's First Machine Learning-Powered Next Generation Firewall

PA-400 Series



PA-460

4.4 Gbps App-ID



PA-450

2.9 Gbps App-ID



PA-445

2.2 Gbps App-ID



PA-440

2.2 Gbps App-ID



PA-415

1.2 Gbps App-ID



PA-410

1.1 Gbps App-ID

PA-1400 Series



PA-1420

9.5 Gbps App-ID



PA-1410

6.8 Gbps App-ID

PA-3400 Series



PA-3440

24 Gbps App-ID



PA-3430

20.5 Gbps App-ID



PA-3420

16.9 Gbps App-ID



PA-3410

11 Gbps App-ID

PA-5400 Series



PA-5440

72 Gbps App-ID



PA-5430

61 Gbps App-ID



PA-5420

56 Gbps App-ID



PA-5410

43.5 Gbps App-ID

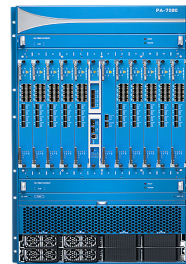
PA-5450



PA-5450

Up to 200 Gbps App-ID

PA-7000 Series



PA-7080

635 Gbps App-ID



PA-7050

384 Gbps App-ID

Small Branches

Network Perimeter

Large Data Centers

Platform

Firewall Types

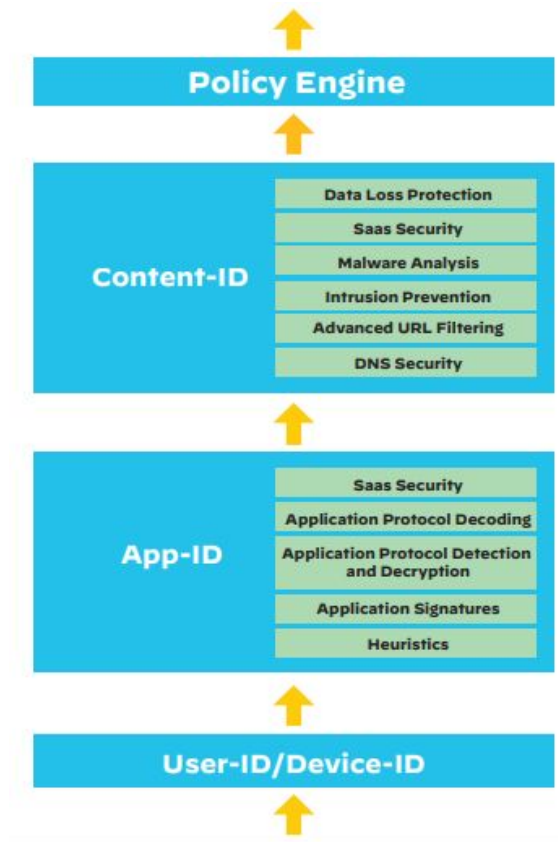
- Physical
 - Subscriptions (CDSS)/Bundles
 - Core Security Bundle
 - Advanced Threat Prevention
 - Advanced Wildfire
 - Advanced URL
 - DNS Security
 - Advanced SD-WAN
 - Globalprotect/Prisma Access Agent
 - Support
- Software (NGFW Credits)
 - On Premise
 - Cloud

Platform

Firewalls: Packet Flow

Single Pass Parallel Processing

Packet Flow Processing



Ways to Manage

Ways to Manage

- Console
- CLI
- Web GUI
- API
- Panorama
- Strata Cloud Manager



Management

Console

Ways to Manage

CLI:

```
admin@PA440-WAN> show interface management
|           Pipe through a command
<Enter>    Finish input
```

```
admin@PA440-WAN> show interface management
```

```
-----
Name: Management Interface
```

```
Link status:
```

```
Runtime link speed/duplex/state: 1000/full/up
```

```
Configured link speed/duplex/state: auto/auto/auto
```

```
MAC address:
```

```
Port MAC address 8c:36:7a:02:c6:46
```

```
Ip address: 192.168.18.13
```

```
Netmask: 255.255.255.0
```

```
Default gateway: 192.168.18.1
```

```
Ipv6 address: unknown
```

```
Ipv6 link local address: fe80::8e36:7aff:fe02:c646/64
```

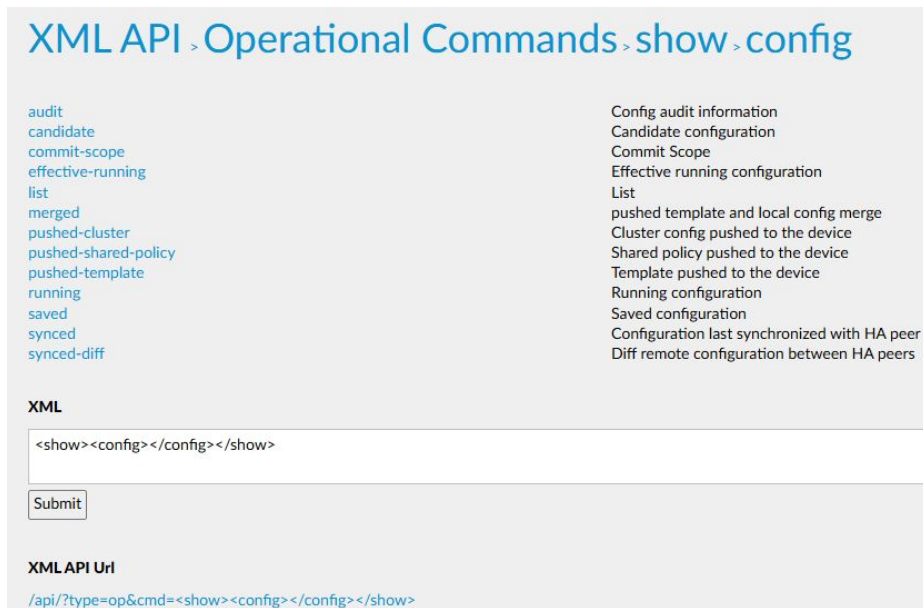
```
Ipv6 default gateway:
```

```
-----
```

Ways to Manage

XML-API:

- You can view the full list of resources in the REST API Reference on the firewall at https://<IP_address>/api



Ways to Manage

Rest-API:

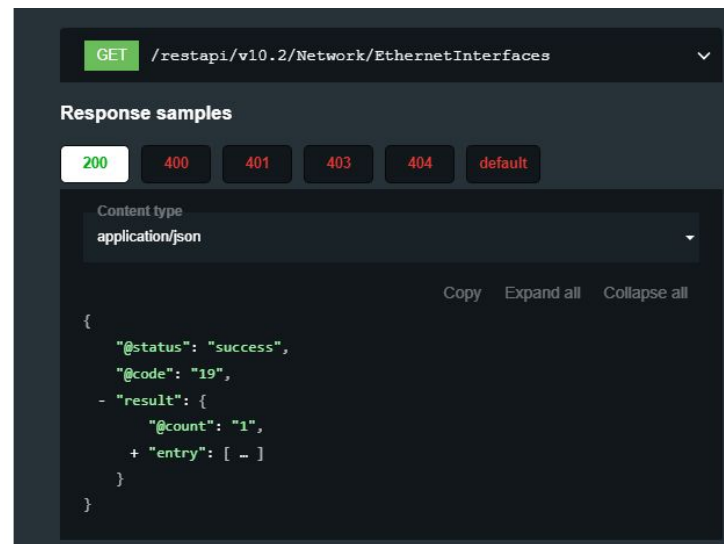
- You can view the full list of resources in the REST API Reference on the firewall at https://<IP_address>/restapi-doc.

List Ethernet Interfaces

Get Ethernet Interfaces.

QUERY PARAMETERS

name	string The name of the entry
location	string Value: "panorama-pushed"
output-format	string Default: "json" Enum: "json" "xml" Specify the output format to be JSON or XML. This is equivalent to setting the <code>Accept</code> header to <code>application/json</code> or <code>application/xml</code> . If you include both <code>output-format</code> and <code>Accept</code> header, the value of <code>output-format</code> will override the header.



Configuration Management

Configuration Management

- Candidate Configuration - Configuration before a commit
- Running Configuration - Configuration after a commit

Commit

?

Doing a commit will overwrite the running configuration with the commit scope.

☒ Commit All Changes ☐ Commit Changes Made By: 1 admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			
▶ device-and-network	Device and Network Configuration			

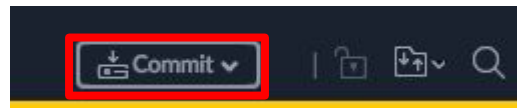
Preview Changes

Change Summary

Validate Commit

Note: This shows all the changes in login admin's accessible domain.

Description



Configuration Management

- Commit All Changes
- Commit Changes Made by current user

Commit

Doing a commit will overwrite the running configuration with the commit scope.

☒ Commit All Changes ☐ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▼ policy-and-objects	Policy and Objects			
outside		tag		admin
inside		tag		admin
Allowed URLs		Others		admin
default-1		Others		admin
dmz		tag		admin
Custom-URL-Profile		Others		admin
► device-and-network	Device and Network Configuration			

Configuration Management

 Preview Changes  Change Summary  Validate Commit

Note: This shows all the changes in login admin's accessible domain.

Description

Recommended

Device Config Audit (WAN-VM)

Wed Jan 24 14:27:33 CST 2024

Legend: Added Modified Deleted

Local Device Changes	
Running Configuration	Candidate Configuration
260 dampening-profile {	260 dampening-profile {
261 default {	261 default {
262 cutoff 1.25;	262 cutoff 1.25;
263 reuse 0.5;	263 reuse 0.5;
264 max-hold-time 900;	264 max-hold-time 900;
265 decay-half-life-reachable 300;	265 decay-half-life-reachable 300;
266 decay-half-life-unreachable 900;	266 decay-half-life-unreachable 900;
267 enable yes;	267 enable yes;
268 }	268 }
269 }	269 }
 	270 routing-options {
 	271 graceful-restart {
 	272 enable yes;
 	273 }
 	274 }
 	275 }
 	276 rip {
 	277 enable no;
 	278 }
 	279 ospf {
 	280 enable no;

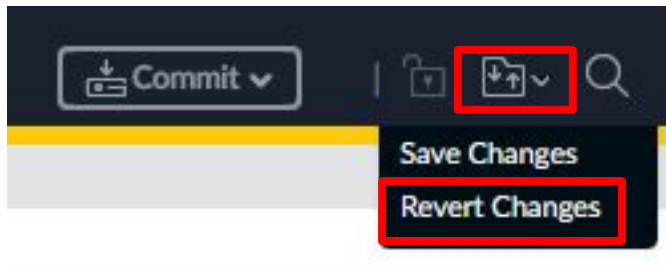
Preview Changes

Lines of Context 10

Configuration Management

Revert candidate configuration changes:

- Remove changes made to the candidate configuration
- This is done before you commit changes



Configuration Management

Backing up a configuration:

The screenshot shows the Palo Alto VM configuration management interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE' (highlighted with a red box). The left sidebar contains a 'Setup' menu (highlighted with a red box) with options like High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, IoT, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management, and Certificates. The main content area is titled 'Configuration Management' and has a sub-menu with 'Management', 'Operations' (highlighted with a red box), 'Services', 'Interfaces', 'Telemetry', 'Content-ID', 'WildFire', and 'Session'. Under the 'Operations' sub-menu, there are several actions: 'Revert' (Revert to last saved configuration, Revert to running configuration), 'Save' (Save named configuration snapshot - highlighted with a cyan box, Save candidate configuration), 'Load' (Load named configuration snapshot, Load configuration version), 'Export' (Export named configuration snapshot - highlighted with a red box, Export configuration version, Export device state), and 'Import' (Import named configuration snapshot, Import device state). To the right of the 'Save named configuration snapshot' option, the text 'Save a configuration by name' is displayed. To the right of the 'Export named configuration snapshot' option, the text 'Export the running or named configuration' is displayed.

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Setup

- High Availability
- Config Audit
- Password Profiles
- Administrators
- Admin Roles
- Authentication Profile
- Authentication Sequence
- User Identification
- IoT
- Data Redistribution
- Device Quarantine
- VM Information Sources
- Troubleshooting
- Certificate Management
- Certificates

Management **Operations** Services Interfaces Telemetry Content-ID WildFire Session

Configuration Management

Revert Revert to last saved configuration
Revert to running configuration

Save **Save named configuration snapshot** Save a configuration by name
Save candidate configuration

Load Load named configuration snapshot
Load configuration version

Export **Export named configuration snapshot** Export the running or named configuration
Export configuration version
Export device state

Import Import named configuration snapshot
Import device state

Configuration Management

Restore a configuration:

The screenshot shows the Palo Alto VM configuration management interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE' (highlighted with a red box). The left sidebar contains a 'Setup' menu (highlighted with a red box) with options like High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, IoT, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management, and Certificates. The main content area is titled 'Configuration Management' and has sub-tabs: 'Management', 'Operations' (highlighted with a red box), 'Services', 'Interfaces', 'Telemetry', 'Content-ID', 'WildFire', and 'Session'. Under the 'Operations' tab, there are several actions: 'Revert' (Revert to last saved configuration, Revert to running configuration), 'Save' (Save named configuration snapshot, Save candidate configuration), 'Load' (Load named configuration snapshot - highlighted with a red box, Load configuration version), 'Export' (Export named configuration snapshot, Export configuration version, Export device state), and 'Import' (Import named configuration snapshot - highlighted with a cyan box, Import device state). To the right of the 'Load' action, there is a text box: 'Load a configuration into the current candidate configuration'. To the right of the 'Import' action, there is a text box: 'Imports a named configuration (change name if running-config.xml)'.

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Setup

- High Availability
- Config Audit
- Password Profiles
- Administrators
- Admin Roles
- Authentication Profile
- Authentication Sequence
- User Identification
- IoT
- Data Redistribution
- Device Quarantine
- VM Information Sources
- Troubleshooting
- Certificate Management
- Certificates

Management **Operations** Services Interfaces Telemetry Content-ID WildFire Session

Configuration Management

Revert Revert to last saved configuration
Revert to running configuration

Save Save named configuration snapshot
Save candidate configuration

Load **Load named configuration snapshot**
Load configuration version

Export Export named configuration snapshot
Export configuration version
Export device state

Import **Import named configuration snapshot**
Import device state

Load a configuration into the current candidate configuration

Imports a named configuration (change name if running-config.xml)

Configuration Management

XML vs Set view:

- Exported configurations are in XML format
- [XML Basics](#)
- Set commands are used to configure a firewall via CLI or Console

View the configuration as a set command or XML format in the CLI or Console:

- "set" format: > set cli config-output-format set
- "xml" format: > set cli config-output-format xml

Configuration Management

XML Format (default)

```
admin@PA440-WAN# show
deviceconfig {
  system {
    hostname PA440-WAN;
    timezone US/Central;
    login-banner "You have accessed a protected system. Log off immediately if you are not an authorized user.";
    ntp-servers {
      primary-ntp-server {
        ntp-server-address 0.pool.ntp.org;
      }
      secondary-ntp-server {
        ntp-server-address 1.pool.ntp.org;
      }
    }
    snmp-setting {
      access-setting {
        version {
          v3;
        }
      }
    }
    update-schedule {
      threats {
        recurring {
          every-30-mins {
            at 2;
            action download-and-install;
          }
        }
      }
    }
  }
}
```

Configuration Management

Set command format:

```
admin@PA440-WAN# show
set deviceconfig system hostname PA440-WAN
set deviceconfig system timezone US/Central
set deviceconfig system login-banner "You have accessed a protected system. Log off immediately if you are not an authorized user."
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address 0.pool.ntp.org
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address 1.pool.ntp.org
set deviceconfig system snmp-setting access-setting version v3
set deviceconfig system update-schedule threats recurring every-30-mins at 2
set deviceconfig system update-schedule threats recurring every-30-mins action download-and-install
set deviceconfig system update-schedule threats recurring threshold 48
```

Initial Configuration

Initial Configuration

Management Interface Configuration:

- Default IP Address 192.168.1.1/24

Static IP Address

- Set new IP Address and Netmask
- Set Default-Gateway
- Set DNS Servers

DHCP IP Address

- Receive all information from a DHCP Server

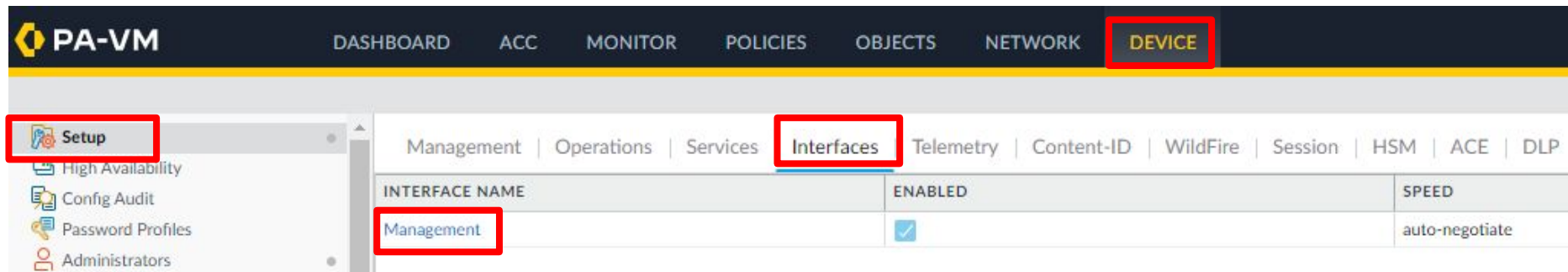
Initial Configuration

CLI Configuration for Static IP Address on Management Interface:

```
configure
set deviceconfig system type static
set deviceconfig system ip-address <IP_Address> netmask <Net_Mask>
set deviceconfig system default-gateway <Gateway>
set deviceconfig system dns-setting servers primary <dns-server>
set deviceconfig system dns-setting servers secondary <dns-server>
commit
exit
```

Initial Configuration

GUI Configuration for Management Interface:



The screenshot displays the Palo Alto Networks PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and **DEVICE**. The left sidebar shows the Setup menu with sub-items: High Availability, Config Audit, Password Profiles, and Administrators. The main content area is divided into tabs: Management, Operations, Services, **Interfaces**, Telemetry, Content-ID, WildFire, Session, HSM, ACE, and DLP. The Interfaces tab is active, showing a table with the following data:

INTERFACE NAME	ENABLED	SPEED
Management	☒	auto-negotiate

Initial Configuration

Management Interface Settings

IP Type ☒ Static ☐ DHCP Client

IP Address 192.168.18.31

Netmask 255.255.255.0

Default Gateway 192.168.18.1

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed auto-negotiate

MTU 1500

Administrative Management Services

☐ HTTP

☐ Telnet

☒ HTTPS

☒ SSH

Network Services

☐ HTTP OCSP

☐ SNMP

☐ User-ID Syslog Listener-SSL

☒ Ping

☐ User-ID

☐ User-ID Syslog Listener-UDP

Initial Configuration

The screenshot displays the Palo Alto VM configuration interface. The top navigation bar includes the following tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and **DEVICE** (highlighted with a red box). On the left sidebar, the **Setup** menu item is highlighted with a red box. The main content area shows the **Services** configuration page, which is also highlighted with a red box. The **Services** page includes a sub-tab bar with Management, Operations, **Services** (highlighted), Interfaces, Telemetry, Content-ID, and WildFire. The **Services** configuration table lists the following settings:

Configuration Item	Value
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	☒
DNS Servers	
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Minimum FQDN Refresh Time (sec)	30
FQDN Stale Entry Timeout (min)	1440
Proxy Server	
Primary NTP Server Address	0.pool.ntp.org
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	1.pool.ntp.org
Secondary NTP Server Authentication Type	None

Initial Configuration

Services

Services

NTP

Update Server



Verify Update Server Identity

DNS Settings

DNS



Servers



DNS Proxy Object

Primary DNS Server

8.8.8.8

Secondary DNS Server

8.8.4.4

Minimum FQDN Refresh Time (sec)

30

FQDN Stale Entry Timeout (min)

1440

Services



Services

NTP

Primary NTP Server

NTP Server Address

0.pool.ntp.org

Authentication Type

None

Secondary NTP Server

NTP Server Address

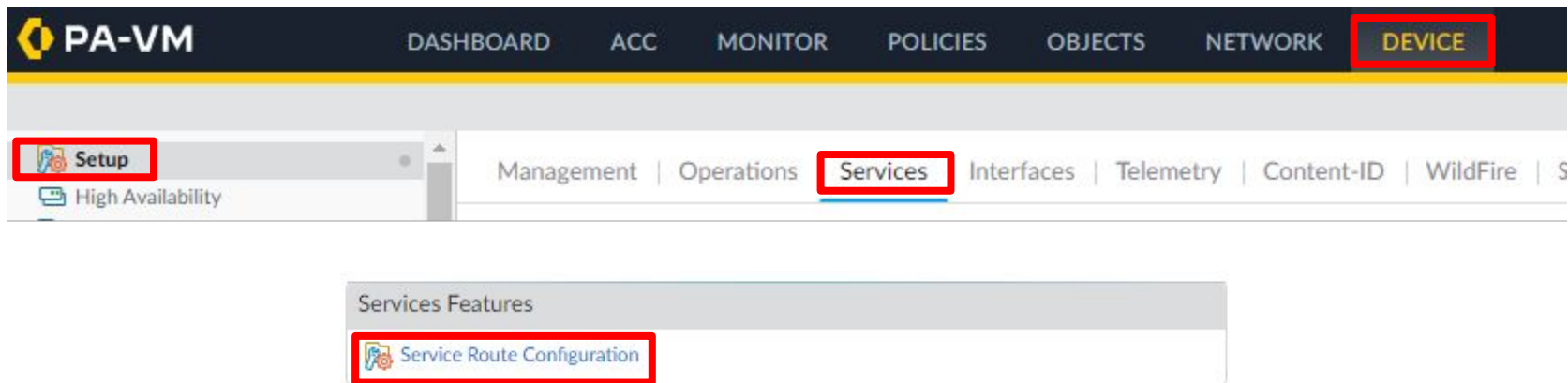
1.pool.ntp.org

Authentication Type

None

Initial Configuration

Service Routes:



Initial Configuration

Service Route Configuration

 Use Management Interface for all

Customize

IPv4

IPv6

Destination

☐	SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
☐	AutoFocus	Use default	Use default
☐	CRL Status	Use default	Use default
☐	Data Services	Use default	Use default
☐	DDNS	Use default	Use default
☐	Panorama pushed updates	Use default	Use default
☐	DNS	Use default	Use default
☐	External Dynamic Lists	Use default	Use default
☐	Email	Use default	Use default
☐	HSM	Use default	Use default
☐	HTTP	Use default	Use default
☐	IoT	Use default	Use default
☐	Kerberos	Use default	Use default

Set Selected Service Routes

OK

Cancel

Service Route Source

Service

dns

Source Interface

Use default

Source Address

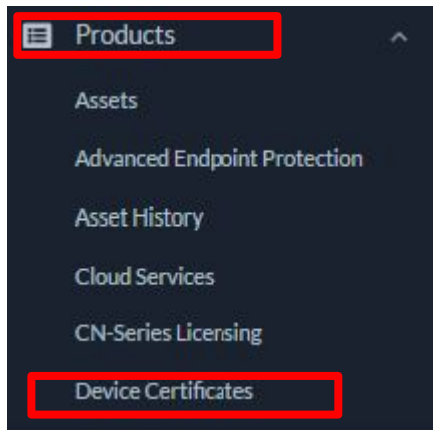
Use default

OK

Cancel

Initial Configuration

Device Certificate:



One Time Password

Choose the "One-Time Password" option if:

1. You are manually managing the Firewalls (Hardware/VM-Series).
2. You are using the Panorama to manage the Firewalls (Hardware/VM-Series).
3. You have Panorama (Hardware/VM-Series).

[View OTP History](#)

[Generate OTP](#)

Initial Configuration

Device Number

☒ Generate OTP for a Next-Gen Firewall (PanOS)

☐ Generate OTP for a Panorama

☐ Generate OTP for Panorama managed devices

☐ Generate OTP for WF-500 devices

Cancel

Next

Generate OTP for a Next-Gen Firewall (PanOS)

OTP provides users the password to input into the PAN-OS device.

This is a required step to enable secured use of the PAN-OS device for some functions.

The password is valid for a limited time.

If the time expires before you use this password, please generate a new password.

* PAN-OS Device :

Select a device

▼

Cancel

Back

Generate OTP

Initial Configuration

Your one time password has been created and is available below. The password will be valid for 60 minutes.

PAN OS Device:

Password:

Expires On: 5/23/2023 5:54:37 PM

Generate OTP

Download OTP

Copy to Clipboard

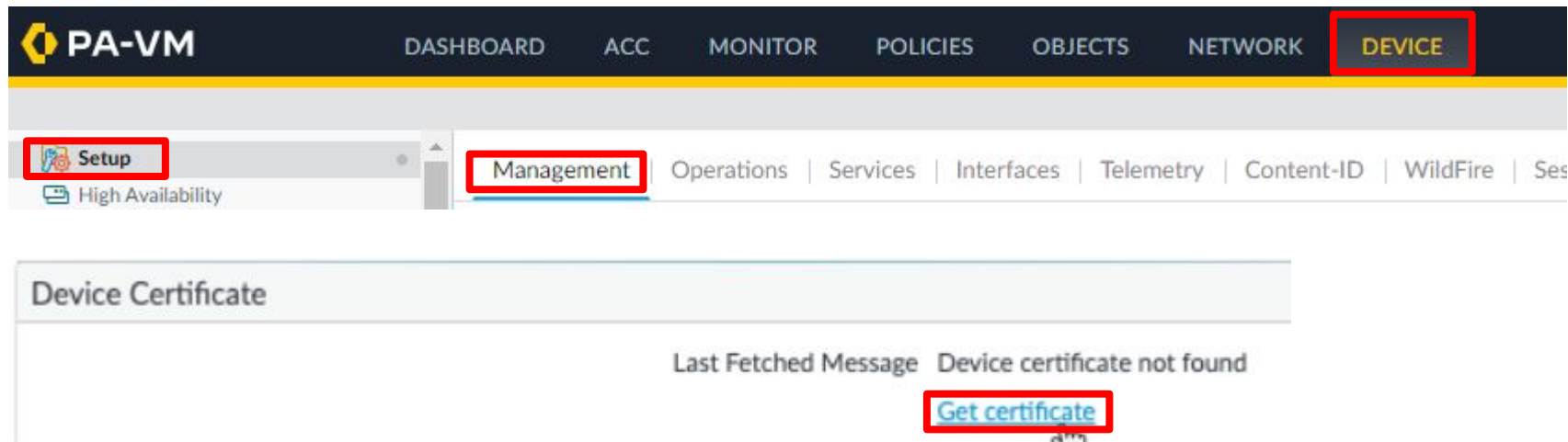
Done

Initial Configuration

Import the OTP: CLI

You can also install the device certificate from the **firewall CLI** using the command:

```
admin>request certificate fetch otp <otp_value>
```



Initial Configuration

Device Certificate Validation:

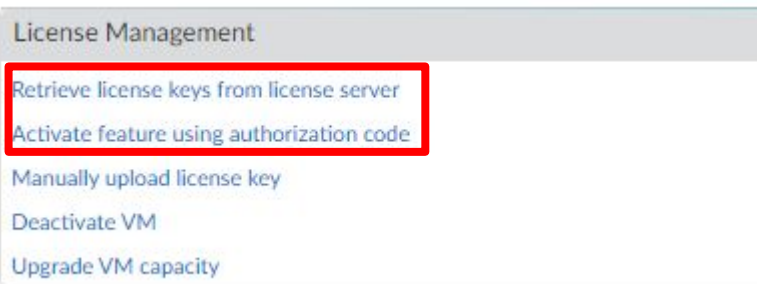
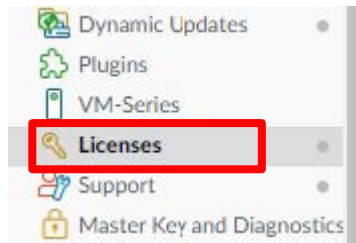
The screenshot displays the Palo Alto Networks PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and **DEVICE**. On the left sidebar, the **Setup** menu is expanded, showing **Management** as the selected option. The main content area is titled "Device Certificate" and displays the following information:

Current Device Certificate Status	Valid
Not Valid Before	2023/12/08 04:03:49 CST
Not Valid After	2024/03/07 04:03:48 CST
Last Fetched Message	Successfully fetched Device Certificate
Last Fetched Status	success
Last Fetched Timestamp	2023/12/08 04:13:49 CST

A [Get certificate](#) link is located at the bottom of the status section.

Initial Configuration

License the firewall: Device -> Licenses

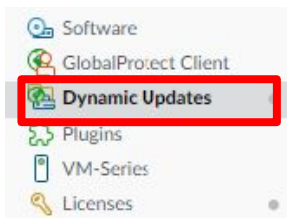


Premium	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	24 x 7 phone support; advanced replacement hardware service

WildFire License	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	WildFire signature feed, integrated WildFire logs, WildFire API

Initial Configuration

Dynamic Updates: Device -> Dynamic Updates



VERSION ^	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
✓ Applications and Threats	Last checked: 2024/01/16 17:04:06 CST Schedule: Every Wednesday at 01:02 (Download only)								
8791-8464	panupv2-all-contents-8791-8464	Apps, Threats	Full	76 MB	e398e1db9b8729...	2023/12/18 15:25:59 CST			Download
8792-8469	panupv2-all-contents-8792-8469	Apps, Threats	Full	76 MB	d1469dd23f5408...	2023/12/19 16:38:55 CST			Download
8793-8478	panupv2-all-contents-8793-8478	Apps, Threats	Full	76 MB	bb01505fbcaaa9e...	2023/12/27 14:33:32 CST			Download
8795-8489	panupv2-all-contents-8795-8489	Apps, Threats	Full	76 MB	717744f8cd8feaa...	2024/01/08 12:26:00 CST			Download
8796-8491	panupv2-all-contents-8796-8491	Apps, Threats	Full	76 MB	917f47a2bda325...	2024/01/09 10:50:27 CST			Download
8797-8498	panupv2-all-contents-8797-8498	Apps, Threats	Full	77 MB	b996d57bf5d3c1...	2024/01/12 14:58:30 CST			Download
✓ GlobalProtect Clientless VPN	Last checked: 2024/01/16 17:04:12 CST Schedule: None								
98-260	panup-all-gp-98-260	GlobalProtectClientlessV...	Full	77 KB	52ef80beb11d00...	2023/05/22 17:41:22 CDT			Download
✓ Device Dictionary	Last checked: 2024/01/16 17:04:08 CST								
107-458	panup-all-deviceid-107-458	IoT	Full	204 KB	ef96b8a528944f7...	2023/12/22 17:14:26 CST			
108-460	panup-all-deviceid-108-460	IoT	Full	204 KB	9f2fe8468061f71...	2023/12/29 13:37:56 CST			
109-462	panup-all-deviceid-109-462	IoT	Full	204 KB	91819e632a9396...	2024/01/04 16:31:12 CST			
110-464	panup-all-deviceid-110-464	IoT	Full	205 KB	301b6a5e18080c...	2024/01/11 10:28:40 CST			
✓ WildFire	Last checked: 2024/01/16 17:04:11 CST Schedule: None								
839107-842935	panupv3-all-wildfire-839107-842935	PAN OS 10.0 And Later	Full	8 MB	885442387929f7...	2024/01/16 17:02:14 CST			Download

Initial Configuration

Dynamic Updates: Device -> Dynamic Updates

1.

DOWNLOADED	CURRENTLY INSTALLED	ACTION
		Download
		Download
		Download
		Download
		Download
✓		Install Review Policies Review Apps Export

2.

✓	✓	Review Policies Review Apps Export
---	---	--

3.

Check Now	Upload	Install From File
-----------	--------	-------------------

VERSION ^	FILE NAME v
Antivirus	Last checked: 2024/01/16 17:14:04 CST Schedule: None
4695-5213	panup-all-antivirus-4695-5213
4696-5214	panup-all-antivirus-4696-5214
4697-5215	panup-all-antivirus-4697-5215
4698-5216	panup-all-antivirus-4698-5216
4699-5217	panup-all-antivirus-4699-5217
Applications and Threats	Last checked: 2024/01/16 17:13:59 CST Sched
8791-8464	panupv2-all-contents-8791-8464
8792-8469	panupv2-all-contents-8792-8469
8793-8478	panupv2-all-contents-8793-8478
8795-8489	panupv2-all-contents-8795-8489
8796-8491	panupv2-all-contents-8796-8491
8797-8498	panupv2-all-contents-8797-8498

Interfaces

Interfaces

Interface Types:

- Tap
- Virtual Wire
- Layer 2
- Layer 3
- Aggregate Ethernet
- HA
- Decrypt Mirror

Interfaces

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Interfaces

Zones

VLANs

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

DNS Proxy

Proxy

GlobalProtect

Portals

Gateways

MDM

Clientless Access

Ethernet

VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1				none	none	Untagged	none	none
ethernet1/2				none	none	Untagged	none	none
ethernet1/3				none	none	Untagged	none	none
ethernet1/4				none	none	Untagged	none	none
ethernet1/5				none	none	Untagged	none	none
ethernet1/6				none	none	Untagged	none	none

Interfaces

Tap Interface:

Ethernet Interface

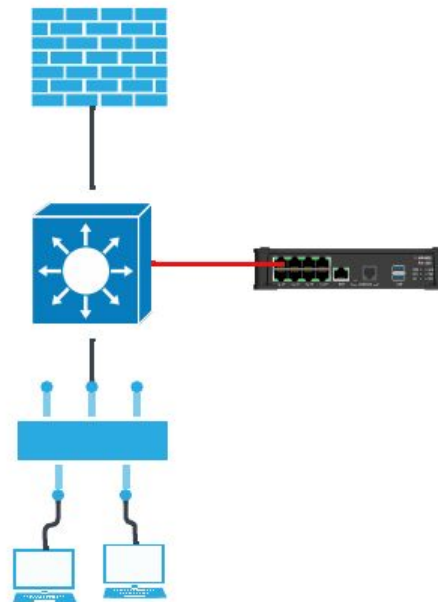
Interface Name	ethernet1/7
Comment	
Interface Type	Tap
Netflow Profile	None

Config | Advanced

Assign Interface To

Security Zone	None
---------------	------

Add a Zone for the interface



Interfaces

vWire Interface:

Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

Config | Advanced

Assign Interface To

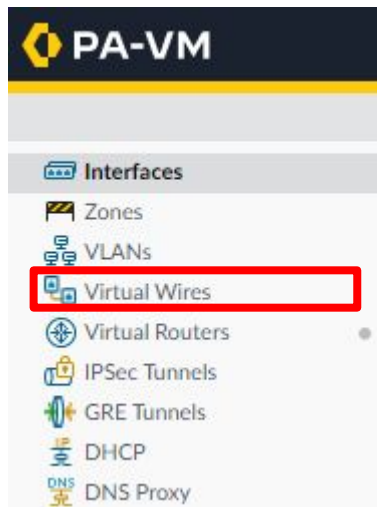
Virtual Wire	None
Security Zone	None
New Virtual Wire	

Add a Zone for the interface



Interfaces

vWire Interface:



The screenshot shows the 'Virtual Wire' configuration page. The page has a title bar 'Virtual Wire' with a help icon. Below the title bar, there are several configuration fields:

- Name:** A text input field, highlighted with a red box.
- Interface1:** A dropdown menu showing 'None', highlighted with a red box.
- Interface2:** A dropdown menu showing 'None', highlighted with a red box.
- Tag Allowed:** A text input field containing '[0 - 4094]'.

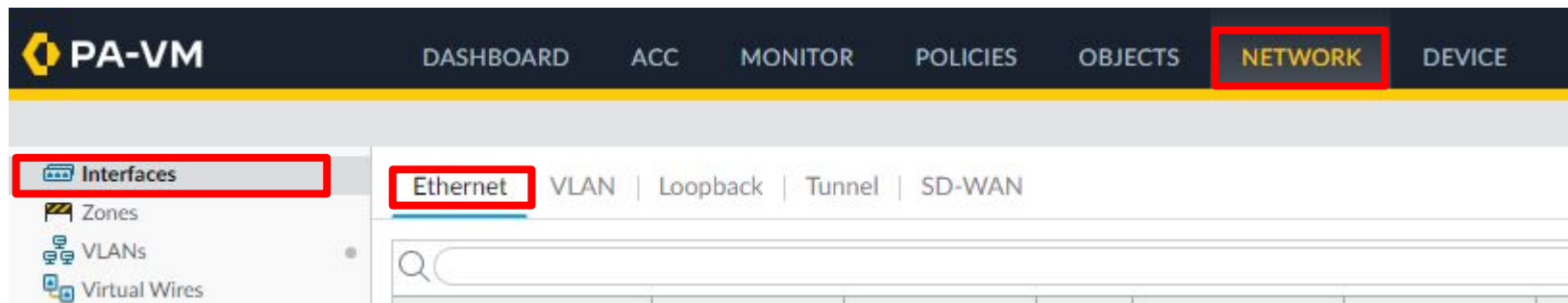
Below the 'Tag Allowed' field, there is a descriptive text: 'Enter either integers (e.g. 10) or ranges (100-200) separated by commas. Integer values can be between 0 and 4094.'

At the bottom, there are two checkboxes:

- ☐ Multicast Firewalling
- ☒ Link State Pass Through

Interfaces

Layer 2 Interface:



Interfaces

Layer 2 Interface: Single VLAN

Ethernet Interface

Interface Name

ethernet1/5

Comment

Interface Type

Layer2

Netflow Profile

None

Config

Advanced

Assign Interface To

VLAN

VLAN10

Security Zone

None

VLAN10

New VLAN

OK

Cancel

Interfaces

Layer 2 Interface: Multiple VLANs

Select the Interface and at the bottom of the page select: + Add Subinterface

Layer2 Subinterface ?

Interface Name

ethernet1/5

10

Comment

Tag

10

Netflow Profile

None

▼

Assign Interface To

VLAN

VLAN10

▼

Security Zone

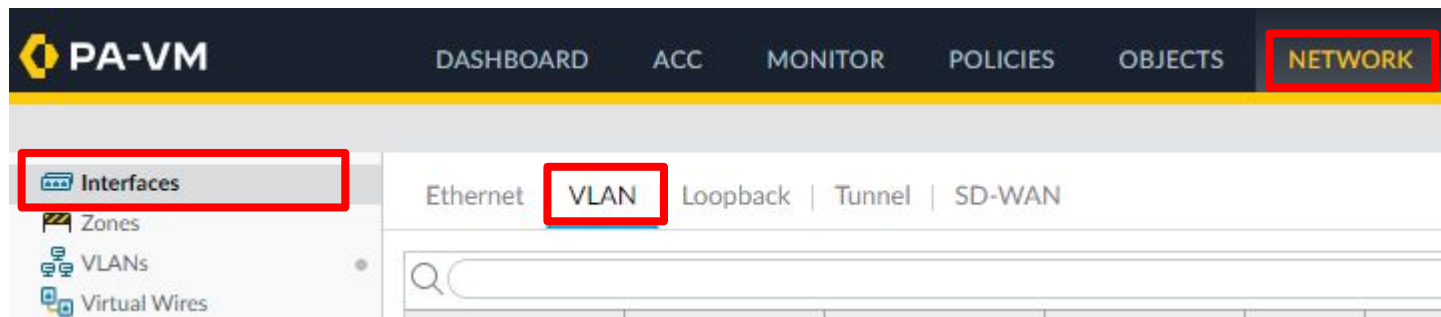
None

▼

ethernet1/5	▼	Layer2		none	none	Untagged	none
ethernet1/5.10		Layer2		none	none	10	VLAN10

Interfaces

Layer 2 Interface: VLAN Interface



Interfaces

Layer 2 Interface: VLAN Interface

VLAN Interface

?

Interface Name

vlan

10

Comment

Netflow Profile

None

▼

Config

IPv4

IPv6

Advanced

Assign Interface To

VLAN

VLAN10

▼

Virtual Router

None

▼

Security Zone

None

▼

OK

Cancel

Interfaces

Layer 2 Interface: VLAN Interface

VLAN Interface

Interface Name

vlan

.

10

Comment

Netflow Profile

None

▼

Config

IPv4

IPv6

Advanced

Type

☒ Static

☐ DHCP Client

☐

IP

☒

10.0.1.1/24

▼

New  Address

+

Add

-

Delete

↑

Move Up

↓

Move Down

IP address/netmask. Ex. 192.168.2.254/24

Interfaces

Layer 3 Interface:

Ethernet Interface

Interface Name

ethernet1/5

Comment

Interface Type

Layer3

Netflow Profile

None

Config

IPv4

IPv6

SD-WAN

Advanced

Assign Interface To

Virtual Router

None

Security Zone

None

OK

Cancel

Add a Zone and VR for
the interface

Interfaces

Layer 3 Interface:

Ethernet Interface



Interface Name ethernet1/5

Comment

Interface Type Layer3

Netflow Profile None

Config

IPv4

IPv6

SD-WAN

Advanced

☐ Enable SD-WAN

Type ☒ Static ☐ PPPoE ☐ DHCP Client



IP



10.0.1.1/24



New Address



Add



Delete



Move Up



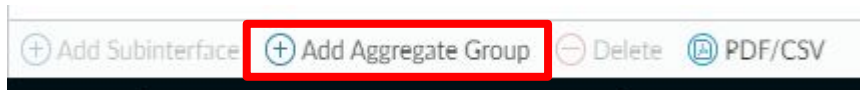
Move Down

Interfaces

Port Aggregation:

Needs to be Physical hardware.

Select the interfaces you want to aggregate.



Interfaces

Port Aggregation:

Aggregate Ethernet Interface

Interface Name

ae

1

Comment

Interface Type

Layer3

Netflow Profile

None

Config

IPv4

IPv6

LACP

SD-WAN

Advanced

Assign Interface To

Virtual Router

None

Security Zone

None

Add a Zone and VR
for the interface

Interfaces

Port Aggregation:

Config | IPv4 | IPv6 | **LACP** | SD-WAN | Advanced

☒ Enable LACP

Mode ☒ Passive ☐ Active

Transmission Rate ☐ Fast ☒ Slow

☐ Fast Failover

System Priority

32768

Maximum Interfaces

8

Interfaces

Port Aggregation:

Ethernet Interface ⓘ

Interface Name

ethernet1/4

Comment

Interface Type

Aggregate Ethernet

▼

Aggregate Group

▼

Advanced

Link Settings

Link Speed

auto

▼

Link Duplex

auto

▼

Link State

auto

▼

LACP Port Priority

32768

Interfaces

Interface Management Profiles:

1. The screenshot shows the top navigation bar of the Palo Alto Networks management console. It contains several tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The 'NETWORK' tab is highlighted with a red rectangular box.
2. The screenshot shows a dropdown menu titled 'Network Profiles'. It lists several options: GlobalProtect IPsec Crypto, IKE Gateways, IPsec Crypto, IKE Crypto, Monitor, Interface Mgmt, and Zone Protection. The 'Interface Mgmt' option is highlighted with a red rectangular box.
3. The screenshot shows a row of four buttons: '+ Add', '- Delete', 'Clone', and 'PDF/CSV'. The '+ Add' button is highlighted with a red rectangular box.

Interfaces

Interface Management Profiles:

Interface Management Profile

Name

Administrative Management Services

☐ HTTP

☐ HTTPS

☐ Telnet

☐ SSH

Network Services

☐ Ping

☐ HTTP OCSP

☐ SNMP

☐ Response Pages

☐ User-ID

☐ User-ID Syslog Listener-SSL

☐ User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES

+ Add

- Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6
2001:db8:123:1::1 or 2001:db8:123:1::/64

Interfaces

Interface Management Profile: Apply to the Interface

Ethernet Interface

Interface Name

ethernet1/5

Comment

Interface Type

Layer3

Netflow Profile

None

Config

IPv4

IPv6

SD-WAN

Advanced

Link Settings

Link Speed

auto

Link Duplex

auto

Link State

auto

Other Info

ARP Entries

ND Entries

NDP Proxy

LLDP

DDNS

Cluster

Management Profile

None

MTU

None

☐ Adjust TCP MSS

New Management Profile

IPv4 MSS Adjustment

40

Zones

Zones

Security zones are a logical way to group physical and virtual interfaces on the firewall to control and log the traffic that traverses specific interfaces on your network. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple interfaces of the same type assigned to it (such as tap, layer 2, or layer 3 interfaces), but an interface can belong to only one zone.

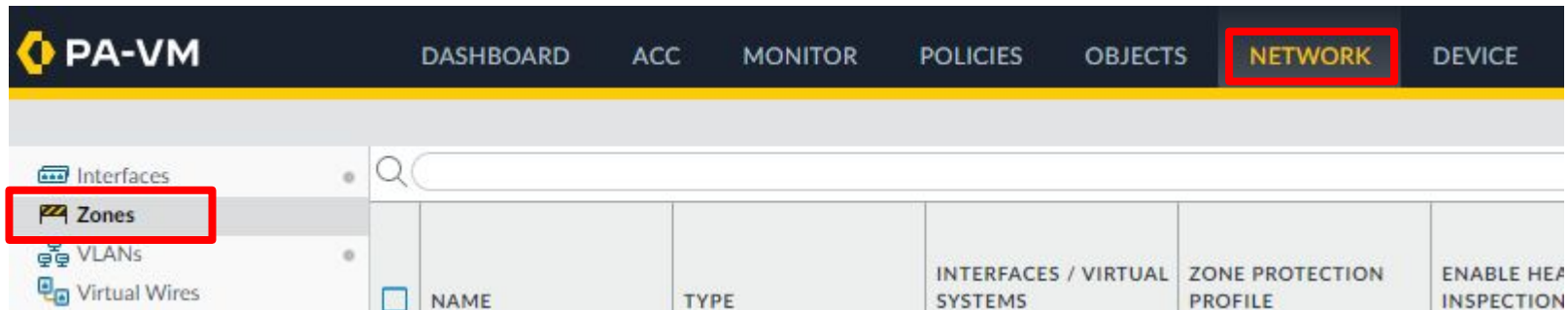
Policy rules on the firewall use security zones to identify where the traffic comes from and where it is going. Traffic can flow freely within a zone but traffic cannot flow between different zones until you define a Security policy rule that allows it. To allow or deny inter-zone traffic, Security policy rules must reference a source zone and destination zone (not interfaces) and the zones must be of the same type; that is, a Security policy rule can allow or deny traffic from one Layer 2 zone only to another Layer 2 zone.

Intrazone - Same Zone

Interzone - Different Zone

Zones

Zones need to match the interfaces they are protecting. (i.e. L3 Zone -> L3 Interface)



The screenshot displays the Palo Alto Networks PA-VM web interface. The top navigation bar includes the PA-VM logo and several tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The NETWORK tab is highlighted with a red box. On the left sidebar, the 'Zones' option is also highlighted with a red box. Below the sidebar, there is a search bar and a table with the following columns: NAME, TYPE, INTERFACES / VIRTUAL SYSTEMS, ZONE PROTECTION PROFILE, and ENABLE HEAT INSPECTION. The table is currently empty.

	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	ENABLE HEAT INSPECTION
--	------	------	------------------------------	-------------------------	------------------------

Zones

Zone

Name

Log Setting

None

Type

Layer3

INTERFACES

+ Add

- Delete

Zone Protection

Zone Protection Profile

None

☒ Enable Packet Buffer Protection

☐ Enable L3 & L4 Header Inspection

User Identification ACL

☐ Enable User Identification

INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add

- Delete

Users from these addresses/subnets will be identified.

EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add

- Delete

Users from these addresses/subnets will not be identified.

Device-ID ACL

☐ Enable Device Identification

INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add

- Delete

Devices from these addresses/subnets will be identified.

EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add

- Delete

Devices from these addresses/subnets will not be identified.

DHCP

DHCP

DHCP Server - Firewall is the source for IP Addressing

DHCP Relay - Firewall relays request to a server on a different subnet

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE

Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy

DHCP Server | DHCP Relay

SEARCH

☐	INTERFACE	MODE	PROE
--------------------------	-----------	------	------

DHCP

DHCP Server

+

Add

−

Delete

PDF/CSV

DHCP Server

Interface

Mode

auto

Lease

Options

☐ Ping IP when allocating new IP

Lease

•

Unlimited

○

Timeout

IP POOLS

192.168.1.20, 192.168.1.0/24 or 192.168.1.10-192.168.1.20

+

Add

−

Delete

RESERVED ADDRESS	MAC ADDRESS	DESCRIPTION
192.168.1.20	xx:xx:xx:xx:xx:xx (Optional MAC Address)	

+

Add

−

Delete

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

DHCP

DHCP Server: Options

DHCP Server

Interface

Mode

Lease

Options

Inheritance Source

Check inheritance source status

Gateway

Subnet Mask

Primary DNS

Secondary DNS

Primary WINS

Secondary WINS

Primary NIS

Secondary NIS

Primary NTP

Secondary NTP

POP3 Server

SMTP Server

DNS Suffix

Custom DHCP options

	NAME	CODE	TYPE	VALUE
--	------	------	------	-------

+ Add

- Delete

↑ Move Up

↓ Move Down

DHCP

DHCP Relay:



DHCP Relay



Interface

☐ IPv4

DHCP SERVER IP ADDRESS

☐ IPv6

DHCP SERVER IPV6 ADDRESS

INTERFACE

Specify outgoing interface when using an IPv6 multicast address for your DHCPv6 server

NAT

NAT

Types of Network Address Translation (NAT) Policies:

Source NAT:

- Static IP - 1-to-1 translation to a defined address
- Dynamic IP - 1-to-1 translation to an address from a pool. Pool should match needs.
- Dynamic IP and Port (DIPP) - 1-to-1 translation to an address from a pool or interface. Pool does not match needs and multiple devices share the same IP and require a different port. Also called Port Address Translation (PAT)

Destination NAT:

- Static IP - 1-to-1 translation to a defined address
- Dynamic IP (with Session Disruption) - 1-to-1 translation to a dynamic IP on the destination device via FQDN.

NAT

NAT Policies:

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Security

NAT

QoS

Policy Based Forwarding

Decryption

NAME

TAGS

SOURCE ZONE

DESTINATION ZONE

DESTINATION INTERFACE

SOURCE

Original Packet

+ Add

- Delete

🔄 Clone

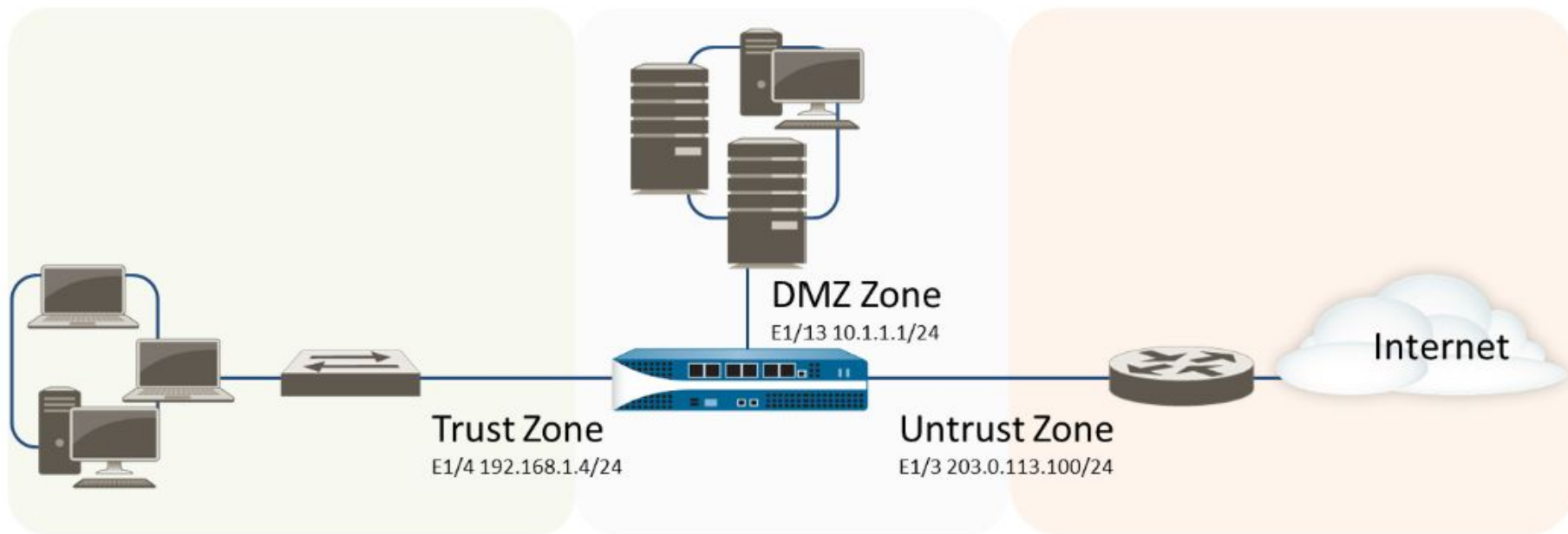
✅ Enable

❌ Disable

Move ▾

NAT

Source NAT:



NAT

Source NAT Example:

NAT Policy Rule

General

Original Packet

Translated Packet

Name

Source NAT 1-1

Description

Tags

Group Rules By Tag

None

NAT Type

ipv4

Audit Comment

[Audit Comment Archive](#)

NAT

Source NAT Example:

NAT Policy Rule ?

General

Original Packet

Translated Packet

☐ Any

☐ SOURCE ZONE ^

☒ Inside

+ Add

- Delete

Destination Zone

Outside

Destination Interface

ethernet1/5

Service

any

☒ Any

☐ SOURCE ADDRESS ^

+ Add

- Delete

☒ Any

☐ DESTINATION ADDRESS ^

+ Add

- Delete

NAT

Source NAT Example:

NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type: **Static IP**

Translated Address: **1.2.3.4**

☐ Bi-directional

Static translation can be to a single address or a subnet of addresses. The subnet will translate to a 1-1 relationship. (i.e. 10.0.0.50 -> 100.0.0.50)

NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type: **Dynamic IP**

☐ TRANSLATED ADDRESS ^

+ Add - Delete

Advanced (Dynamic IP/Port Fallback)

None

Translated Address

Interface Address

None

NAT

Source NAT Example:

NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type **Dynamic IP And Port**

Address Type **Translated Address**

☐ TRANSLATED ADDRESS ^

+ Add - Delete

NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type **Dynamic IP And Port**

Address Type **Interface Address**

Interface **ethernet1/5**

IP Address **1.2.3.1/24**

NAT

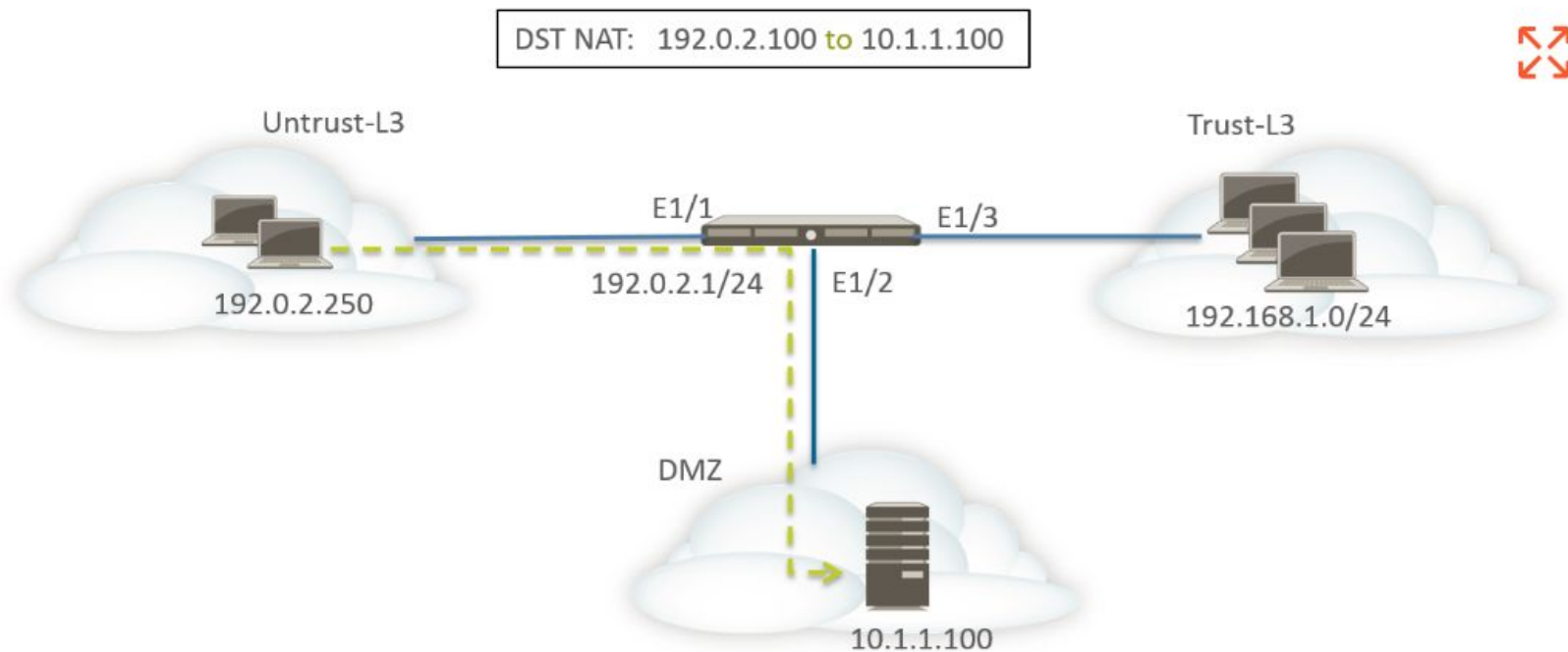
Multiple ISP NAT:

- If you have multiple ISPs, you need multiple NAT policies.

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	ISP-1-NAT-Hub	none	 inside	 outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 10.4.0.2/30	none
2	ISP-2-NAT-Hub	none	 inside	 outside	ethernet1/2	any	any	any	dynamic-ip-and-port ethernet1/2 10.4.1.2/30	none

NAT

Destination NAT:



NAT

Destination NAT Example:

NAT Policy Rule



General

Original Packet

Translated Packet

Name Destination NAT

Description

Tags

Group Rules By Tag

None

NAT Type

ipv4

Audit Comment

[Audit Comment Archive](#)

NAT

Destination NAT Example:

NAT Policy Rule

General

Original Packet

Translated Packet

☐ Any

☐ SOURCE ZONE ^

☒ Outside

Destination Zone

Outside

Destination Interface

any (any interface)

Service

any

+ Add - Delete

☒ Any

☐ SOURCE ADDRESS ^

Destination Address

192.0.2.20/24

+ Add - Delete

NAT

Destination NAT Example:

NAT Policy Rule



General

Original Packet

Translated Packet

Source Address Translation

Translation Type None

Destination Address Translation

Translation Type Static IP

Translated Address 10.1.1.100/24

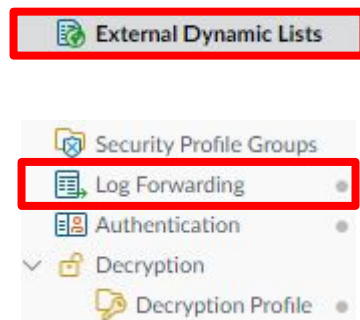
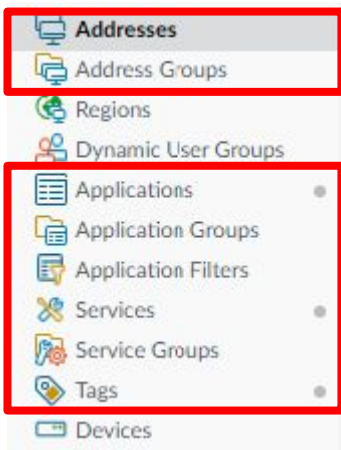
Translated Port [1 - 65535]

☐ Enable DNS Rewrite

Direction reverse

Objects

Objects



Objects

Addresses:

Address

Name

WebServer-Internal

Description

Type

IP Netmask

10.1.1.100/24

Resolve

Tags

Type

IP Netmask

IP Netmask

IP Range

IP Wildcard Mask

FQDN

Objects

Address Groups: Static

Address Group ?

Name

Description

Type

Addresses

☐	ADDRESS ^
☐	ADServer-Internal
☒	WebServer-Internal

Browse Add Delete

Tags

Objects

Address Groups: Dynamic

DAG needs to be used in a Policy to populate.

The screenshot displays the Palo Alto Networks configuration interface for Address Groups. The left pane shows a list of address groups with the following data:

NAME	TYPE	DETAILS
Inside	static	+
Outside	static	+
Servers	static	+
DMZ	static	+

The 'Servers' entry is highlighted with a red box. A green arrow points from this entry to the 'Add Match Criteria' button in the right pane. The right pane shows the configuration for the 'Servers-Dyn' address group:

- Name: Servers-Dyn
- Description:
- Type: Dynamic
- Match: 'Servers'

The 'Add Match Criteria' button is also highlighted with a red box. The 'Tags' section at the bottom shows 'Servers' as a selected tag.

Objects

Addresses and Address Groups Use:

Security Policy Rule

General **Source** Destination Application Service/URL Category Actions

☐ Any	☐ Any	☐ any
☐ SOURCE ZONE ^	☐ SOURCE ADDRESS ^	☐ SOURCE USER ^
☒ Inside	☒ Address ADServer-Internal WebServer-Internal Address Group Servers	

Objects

Tags:

Tag ?

Name **DMZ** ▼

Color any (any zone)

Comments DMZ

Inside

Outside

Zones Automatically populate to create tags

Tag ?

Name Servers ▼

Color ■ Blue ▼

Comments

Ability to create custom tags

Objects

Services:

Service

Name

Corp-RDP

Description

Protocol

☒ TCP ☐ UDP

Destination Port

5389

Source Port

[>= 0]

Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout

☒ Inherit from application ☐ Override

Tags

Objects

Service Groups:

Service Group ?

Name Corp-Svr

☐ SERVICE ^

Tags

Service Group ?

Name Corp-Svr

☐ SERVICE ^

☒

Corp-App

Corp-RDP

service-http

service-https

New  Service  Service Group

Tags

Objects

Service and Service Group Usage:

Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions

select ▼

☐ SERVICE ^

☒ ▼

Service

- service-http
- service-https

New  Service  Service Group

+ Add - Delete

Objects

Applications:

Search dropbox		All	Clear Filters		
CATEGORY ^		SUBCATEGORY ^		RISK ^	TAGS ^
2 business-systems		9 file-sharing		4 1	1 Downloading
1 collaboration		1 office-programs		5 2	1 Editing
1 general-internet		1 storage-backup		3 3	1 Posting
9 saas		2 web-posting		1 4	1 Sharing
					2 Uploading
NAME		CATEGORY	SUBCATEGORY	RISK	TAGS
☐	aerofs	saas	file-sharing	3	Web App
☐	draw.io (1 out of 2 shown)	business-systems	office-programs	2	Web App
☐	draw.io-cloud				
☐	dropbox	saas	file-sharing	4	Web App
☐	dropbox-base				
☐	dropbox-downloading	saas	file-sharing	2	Download... Web App
☐	dropbox-editing	saas	file-sharing	1	Editing Web App
☐	dropbox-lansync-discovery	saas	file-sharing	1	Web App

Objects

Applications:

Application

Name: dropbox-base

Standard Ports: tcp/80,443,17500, udp/17500

Depends on: google-base

Implicitly Uses: ssl, web-browsing

Deny Action: drop-reset

Description:
Dropbox is a file hosting service that offers cloud storage, file synchronization, personal cloud, and client software.

Additional Information: Wikipedia Website Google Yahoo!

Characteristics

Evasive: yes

Excessive Bandwidth Use: no

Used by Malware: no

Capable of File Transfer: yes

Has Known Vulnerabilities: yes

Tunnels Other Applications: no

Prone to Misuse: no

Widely Used: yes

SaaS: yes

Options

TCP Timeout (seconds): 3600

UDP Timeout (seconds): 30

TCP Half Closed (seconds): 120

TCP Time Wait (seconds): 15

App-ID Enabled: yes

Classification

Category: saas

Subcategory: file-sharing

Risk: 4

SaaS Characteristics

Certifications: HIPAA, PCI, SOC I, SOC II, SSAE16

Data Breaches: no

IP Based Restrictions: no

Poor Financial Viability: no

Poor Terms Of Service: no

Tags

Web App

Edit

Objects

Applications: Custom

Application ?

Configuration

Advanced

Signatures

General

Name

Description

Properties

Category

Subcategory

Technology

Parent App

Risk

Characteristics

- | | | |
|---|--|---|
| ☐ Capable of File Transfer | ☐ Has Known Vulnerabilities | ☐ Pervasive |
| ☐ Excessive Bandwidth Use | ☐ Used by Malware | ☐ Prone to Misuse |
| ☐ Tunnels Other Applications | ☐ Evasive | ☐ Continue scanning for other Applications |

Objects

Application: Custom

Application



Configuration

Advanced

Signatures

Defaults

☒ Port ☐ IP Protocol ☐ ICMP Type ☐ ICMP6 Type ☐ None

PORT

[+ Add](#) [- Delete](#)

Enter each port in the form of [tcp|udp]/[dynamic|0-65535] Example: tcp/dynamic or udp/32

Timeouts

Timeout [0 - 604800]

TCP Timeout [0 - 604800]

UDP Timeout [0 - 604800]

TCP Half Closed [1 - 604800]

TCP Time Wait [1 - 600]

Scanning (activated via Security Profiles)

☐ File Types

☐ Viruses

☐ Data Patterns

Objects

Application: Custom

The screenshot displays the Palo Alto Networks configuration interface. On the left, the 'Application' sidebar shows the 'Signatures' tab selected, highlighted with a red box. Below it, a table with columns 'SIGNATURE NAME' and 'COMMENT' is visible. At the bottom of the sidebar, the '+ Add' button is also highlighted with a red box. A green arrow points from this button to the main configuration area. The main area is titled 'Signature' and contains the following fields and options:

- Signature Name:
- Comment:
- Scope: ☒ Transaction ☐ Session
- ☒ Ordered Condition Match

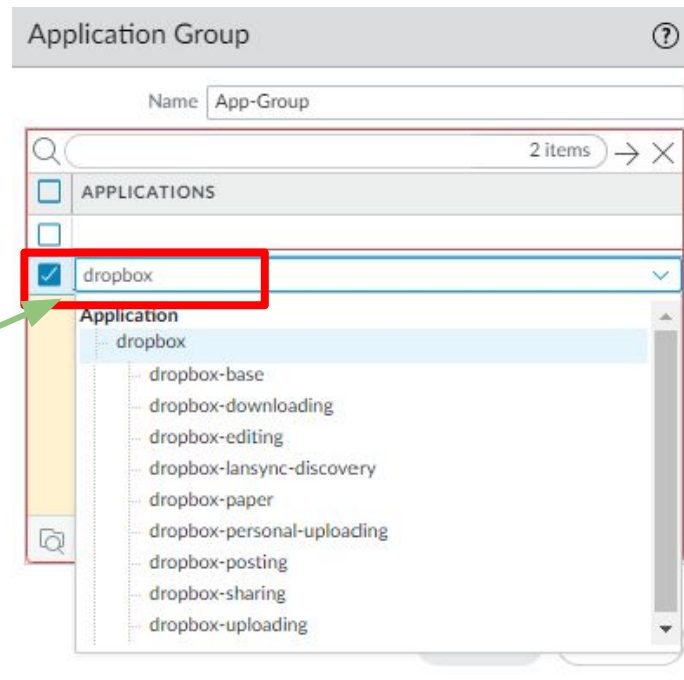
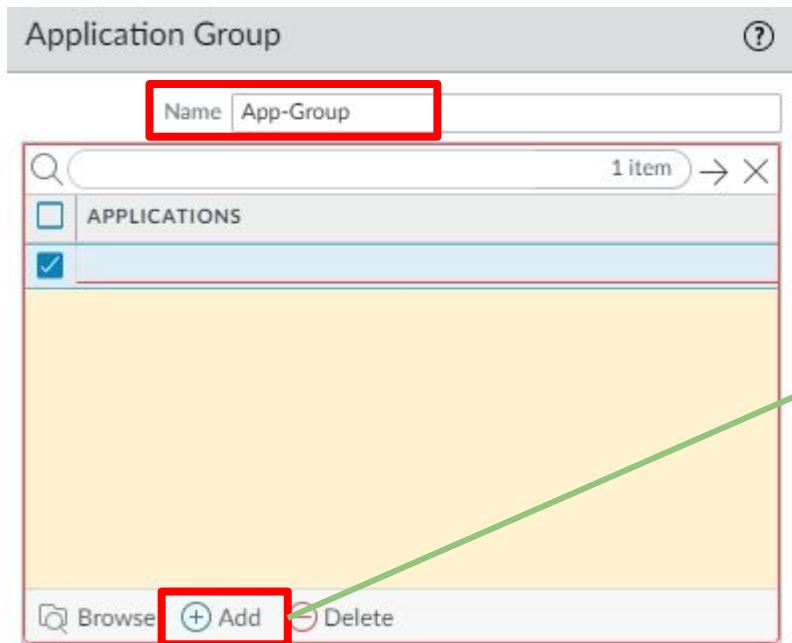
Below these fields is a table with the following headers:

☐	AND CONDITION	COND...	OPERATOR	CONTEXT	PATTERN

At the bottom of the main area, there is a horizontal scrollbar and a row of action buttons: '+ Add Or Condition', '+ Add And Condition', '- Delete', '↑ Move Up', and '↓ Move Down'.

Objects

Application Groups: Static



Objects:

Application Filters: Dynamic

Application Filter

NAME

☐ Apply to New App-IDs only

☒ Clear Filters

4380 matching applications

CATEGORY ^	SUBCATEGORY ^	RISK ^	TAGS ^	CHARACTERISTIC ^
1841 business-systems	26 artificial-intelligence	2253 1	0	36 Data Breaches
456 collaboration	55 audio-streaming	1034 2	App-ID Cloud Engine	646 Evasive
359 general-internet	25 auth-service	580 3	3 Deleting	672 Excessive Bandwidth
339 media	1 collaboration-productivity	370 4	14 DLP App Exclusion	53 FEDRAMP
510 networking	5 content-managemen	143 5	81 Downloading	3 FINRA
873 saas	3 customer-service			117 HIPAA
2 unknown				87 IP Based Restrictions

NAME	CATEGORY	SUBCATEGORY	RISK	TAGS	STANDARD PORTS	EXCLUDE
100bao	general-internet	file-sharing	5		11300,3468,6346,tcp	☒
iec-60870-5-104						☒
104apci-supervisory	business-systems	ics-protocols	2		2404,tcp	☒
104apci-unnumbered	business-systems	ics-protocols	2		2404,tcp	☒
104apci-unnumbered	business-systems	ics-protocols	1		2404,tcp	☒
104apci-unnumbered	business-systems	ics-protocols	1		2404,tcp	☒

Page 1 of 118

Displaying 1 - 84 of 4711

Select what will be used to filter for applications (Category, Subcategory, Risk Level, Tag, Characteristic)

Objects:

External Dynamic Lists: Predefined

☐	NAME	LOCATION	DESCRIPTION	SOURCE
Dynamic IP Lists				
☐	Palo Alto Networks - Tor exit IP addresses	Predefined	IP addresses supplied by multiple providers and validated with Palo Alto Networks threat intelligence data as active Tor exit nodes. Traffic from Tor exit nodes can serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments.	panw-torexip-ip-list
☐	Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	panw-bulletproof-ip-list
☐	Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	panw-highrisk-ip-list
☐	Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	panw-known-ip-list
Dynamic URL Lists				
☐	Palo Alto Networks - Authentication Portal Exclude List	Predefined	Domains and URLs to exclude from Authentication Policy. This list is managed by Palo Alto Networks.	Palo Alto Networks - Authentication Portal Exclude List

Objects:

External Dynamic List: Custom

External Dynamic Lists

Name

Custom-EDL

Create List

List Entries And Exceptions

Type

IP List

Description

Predefined IP List

Predefined URL List

IP List

Domain List

URL List

Subscriber Identity List

Equipment Identity List

Source

Server Authentication

Certificate Profile

Check for updates

Objects:

External Dynamic List: Custom

External Dynamic Lists

Name

Custom-EDL

Create List

List Entries And Exceptions

Type

IP List

Description

Source

http://10.8.6.4/

Server Authentication

Certificate Profile

None

Check for updates

Every five minutes

Objects

Custom EDL:

Lists must be applied to a policy to retrieve information from server.

External Dynamic Lists ⓘ

Name: CINS Army Feed

Create List: **List Entries And Exceptions**

List Entries 15000 items → ×

	LIST ENTRIES
☐	1.10.184.106
☐	1.117.145.83
☐	1.117.204.147
☐	1.117.219.226
☐	1.117.236.166
☐	1.117.91.115
☐	1.119.194.226
☐	1.119.194.226

→

Manual Exceptions 0 items → ×

	LIST ENTRIES
--	--------------

+ Add - Delete

Objects:

Log Forwarding:

☐	NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP
☐	IoT Security Default Profile	Predefined		traffic	All Logs	☒				
				threat	All Logs	☒				
				wildfire	All Logs	☒				
				url	All Logs	☒				
				data	All Logs	☒				
				tunnel	All Logs	☒				
				auth	All Logs	☒				
				decryption	All Logs	☒				

Log Forwarding Profile

Name

Description

0 items

→

×

☐	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS

+

Add

→

Delete

→

Clone

Objects:

Log Forwarding:

Log Forwarding Profile Match List ?

Name

Description

Log Type

Filter

Forward Method

☐ Panorama

☐ SNMP ☐ EMAIL

☐ SYSLOG ☐ HTTP

Built-in Actions

☐ Quarantine

☐ NAME TYPE

Log Type

- traffic
- auth
- data
- decryption
- threat
- traffic
- tunnel
- url
- wildfire

Create a filter to select specific logs

Licenses and Profiles

Licenses

Subscription Licenses and CDSS

- Advanced Threat Prevention
 - Advanced URL Filtering
 - Advanced Wildfire
 - DNS Security - Requires ATP
 - SD-WAN - Requires Panorama
 - GlobalProtect Gateway
 - Internet of Things (IoT) Security
 - Enterprise Data Loss Prevention (DLP)
 - SaaS Security Inline
 - Support
 - Virtual Systems (vSys)
 - Strata Cloud Manager Pro
 - Strata Logging Service (Formally Cortex Data Lake or CDL)
- Part of the Core Security Bundle (CoreSec)

Licenses

What happens when subscriptions expire: [Docs Link](#)

Palo Alto Networks **subscriptions** provide the firewall with added functionality and/or access to a Palo Alto Networks cloud-delivered service. When a license is within 30 days of expiration, a warning message displays in the system log daily until the subscription is renewed or expires. Upon license expiration, some subscriptions continue to function in a limited capacity, and others stop operating completely. Here you can find out what happens when each subscription expires.



The precise moment of license expiry is at the beginning of the following day at 12:00 AM (GMT). For example, if your license is scheduled to end on 1/20 you will have functionality for the remainder of that day. At the start of the new day on 1/21 at 12:00 AM (GMT), the license will expire. All license-related functions operate on Greenwich Mean Time (GMT), regardless of the configured time zone on the firewall.

DNS Security

You can still:

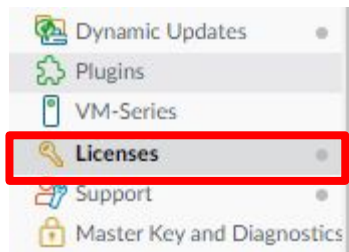
- Use local DNS signatures if you have an active Threat Prevention license.

You can no longer:

- Get new DNS signatures.

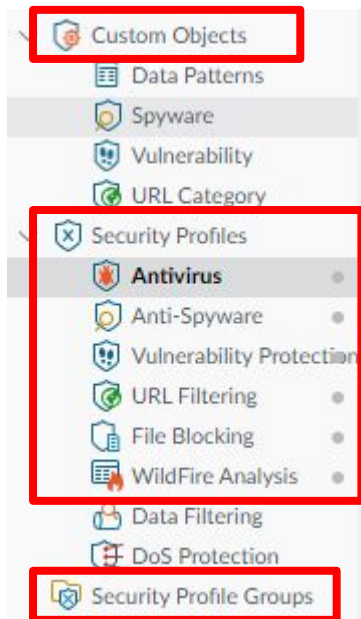
Licenses

Licenses:



Advanced URL Filtering	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	Palo Alto Networks Advanced URL License
DNS Security	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	Palo Alto Networks DNS Security License

Profiles



Profiles

Security Profiles:

- Predefined rules cannot be modified or deleted.
- Rules can be cloned as a starting point for a new custom profile.
- Create a custom profile from scratch.



☐	NAME	LOCATION
☐	default	Predefined
☐	strict	Predefined

Profiles

AntiVirus (ATP): Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads.

☐	NAME	LOCATION	PACKET CAPTURE	HOLD MODE	Decoders			
					PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
☐	default	Predefined	☐	☐	http	default (reset-both)	default (reset-both)	default (reset-both)
					http2	default (reset-both)	default (reset-both)	default (reset-both)
					smtp	default (alert)	default (alert)	default (alert)
					imap	default (alert)	default (alert)	default (alert)
					pop3	default (alert)	default (alert)	default (alert)
					ftp	default (reset-both)	default (reset-both)	default (reset-both)
					smb	default (reset-both)	default (reset-both)	default (reset-both)

Profiles

AntiVirus (ATP):

Antivirus Profile

Name

Custom-AV-Profile

Description

Action

Signature Exceptions

WildFire Inline ML

☐ Enable Packet Capture

☐ Hold for WildFire Real Time Signature Look Up

Decoders

PROTOCOL ^	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	default (reset-both)	default (reset-both)	default (reset-both)
imap	default (alert)	default (alert)	default (alert)
pop3	default (alert)	default (alert)	default (alert)
smb	default (reset-both)	default (reset-both)	default (reset-both)

Application Exceptions

0 items

→ ×

APPLICATION	ACTION
-------------	--------

+ Add

- Delete

default (reset-both)

allow

alert

drop

reset-client

reset-server

reset-both

Profiles

AntiSpyware (ATP): Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.

☐	NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
☐	default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
				simple-high	any	high	default	disable
				simple-medium	any	medium	default	disable
				simple-low	any	low	default	disable
☐	strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
				simple-high	any	high	reset-both	disable
				simple-medium	any	medium	reset-both	disable
				simple-informational	any	informational	default	disable
				simple-low	any	low	default	disable

Profiles

AntiSpyware (ATP): Custom

Anti-Spyware Profile

?

Name

Custom-AS-Profile

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

Inline Cloud Analysis

☐	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
--------------------------	-------------	----------	--------	----------------

+

Add

⊖

Delete

↑

Move Up

↓

Move Down

⌙

Clone

🔍

Find Matching Signatures

Profiles

AntiSpyware (ATP): Custom

Anti-Spyware Policy

Policy Name

Threat Name

any

Used to match any signature containing the entered text as part of the signature name

Category

any

Action

Default

Packet Capture

Default

Severity

☒ any (All severity levels)

☐ critical

☐ high

☐ medium

☐ low

☐ informational

Allow

Alert

Drop

Reset Client

Reset Server

Reset Both

Block IP

Profiles

DNS Security: (ATP and DNS)

Anti-Spyware Profile

Name: Custom-AS-Profile

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

DNS Policies

10 Items

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
Palo Alto Networks Content			
default-paloalto-dns		sinkhole	disable
DNS Security			
Ad Tracking Domains	default (informational)	default (allow)	disable
Command and Control Domains	default (high)	default (block)	disable
Dynamic DNS Hosted Domains	default (informational)	default (allow)	disable
Grayware Domains	default (low)	default (block)	disable
Malware Domains	default (medium)	default (block)	disable
Parked Domains	default (informational)	default (allow)	disable
Phishing Domains	default (low)	default (block)	disable

DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

Block DNS Record Types

☐ SVCB ☐ HTTPS ☐ ANY

default

allow

block

sinkhole

Profiles

Vulnerability Protection ([ATP](#)): Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network.

☐	NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
☐	strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
				simple-client-high	any	client	high	reset-both	disable
				simple-client-medium	any	client	medium	reset-both	disable
				simple-client-informational	any	client	informational	default	disable
				simple-client-low	any	client	low	default	disable
				simple-server-critical	any	server	critical	reset-both	disable
				simple-server-high	any	server	high	reset-both	disable
				more...					
☐	default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable

Profiles

Vulnerability Protection (ATP): Custom

Vulnerability Protection Profile

?

Name

Custom-TP-Profile

Description

Rules

Exceptions

Inline Cloud Analysis

☐	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
--------------------------	-----------	-------------	-----	-----------	----------	--------	----------------

+

Add

-

Delete

↑

Move Up

↓

Move Down

⌕

Clone

🔍

Find Matching Signatures

Profiles

Advanced URL Filtering: URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS. URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS.

☐	NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION
☐	default	Predefined	Allow Categories (59) Alert Categories (6) Continue Categories (0) Block Categories (12) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)

Profiles

URL Filtering: Custom

URL Filtering Profile

Name Custom-URL-Profile

Description

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Inline Categorization

CATEGORY		SITE ACCESS	USER CREDENTIAL SUBMISSION
Pre-defined Categories			
☐	abortion	allow	allow
☐	abused-drugs	allow	allow
☐	adult	allow	allow
☐	alcohol-and-tobacco	allow	allow
☐	artificial-intelligence	allow	allow
☐	auctions	allow	allow

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

alert
allow
block
continue
override

alert
allow
block
continue

Profiles

URL Filtering: Credential Theft Prevention - USER-ID Required

URL Filtering Profile

Name

Custom-URL-Profile

Description

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Inline Categorization

User Credential Detection

Disabled

Disabled

Use IP User Mapping

Use Domain Credential Filter

Use Group Mapping

Profiles

Advanced WildFire: Use a WildFire analysis profile to enable forwarding of unknown files or email links for WildFire analysis.

WildFire Analysis Profile (Read Only) ?

Name default

Description

1 item → ×

☐	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
☐	default	any	any	both	public-cloud

+ Add

- Delete

Profiles

File Blocking Profile:

- Blocks upload and download of PE files (.scr, .cpl, .dll, .ocx, .pif, .exe), Java files (.class, .jar), Help files (.chm, .hlp) and other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat.

☐	NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES
☐	basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types	any any any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf encrypted-rar, encrypted-zip any

- Blocks the same file types as the other profile, and additionally blocks flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files.

☐	strict file blocking	Predefined	Block all risky file types Block encrypted files Log all other file types	any any any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf encrypted-rar, encrypted-zip any
--------------------------	----------------------	------------	---	-------------------	---

Profiles

Security Profile Groups:

Security Profile Group ?

Name	Outbound-Profile-Group
Antivirus Profile	default
Anti-Spyware Profile	strict
Vulnerability Protection Profile	strict
URL Filtering Profile	default
File Blocking Profile	basic file blocking
Data Filtering Profile	None
WildFire Analysis Profile	default

WildFire Analysis Profile

default

None

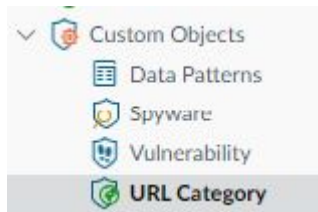
default

New WildFire Analysis

Profiles

Custom Objects:

- Data Patterns - Defines patterns used in Data Filtering profile
- Spyware - Create custom signatures to use in a AS profile
- Vulnerability - Create custom signatures to use in a VP profile
- URL Category - Create custom URL categories to use in a URL Filtering profile



Profiles

Custom Objects: URL Category

Custom URL Category

?

Name

Allowed URLs

Description

Type

URL List

▼

Matches any of the following URLs, domains or host names

🔍

1 item → ✕

☐

SITES

☒

www.facebook.com

⊕ Add

⊖ Delete

|

📄 Import

📄 Export

Profiles

Custom Object: URL Category (Automatically added to a custom profile)

URL Filtering Profile



Name Custom-URL-Profile

Description

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Inline Categorization

78 items → ×			
☐	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
☐	Custom URL Categories		
☐	Allowed URLs *	none	none
☐	Pre-defined Categories		
☐	abortion	allow	allow
☐	abused-drugs	block	block

Security Policies

Security Policies

Security Policies:

- Only intrazone traffic is allowed by default.
- All other traffic is denied.

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Security

NAT

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

</

	NAME
1	intrazone-default
2	interzone-default

ACTION
✓ Allow
✗ Deny

Security Policies

Parts of a rule:

- Required
 - Name
 - Rule Type
 - Source Zone
 - Destination Zone
 - Application
 - Action
- Optional
 - Tag
 - Description
 - Source Address
 - Destination Address
 - URL / URL Category
 - Service
 - Security Profile
 - Options

Security Policies

Security Policy Actions:

ACTION	DESCRIPTION
Allow (default)	Allows the traffic.
Deny	Blocks traffic and enforces the default Deny Action defined for the application that is being denied.
Drop	Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset isn't sent to the host/application. For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: Drop and enable the Send ICMP Unreachable check box. When enabled, the ICMP code is sent for communication with the destination is administratively prohibited—ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.
Reset client	Sends a TCP reset to the client-side device.
Reset server	Sends a TCP reset to the server-side device.
Reset both	Sends a TCP reset to both the client-side and server-side devices.

Security Policies

Create a new policy:

Security Policy Rule

General

Source

Destination

Application

Service/URL Category

Actions

Name

Rule Type

Description

Tags

Group Rules By Tag

Audit Comment

universal (default)

None

Audit Comment Archive

universal (default)

intrazone

interzone

Recommended

Security Policies

Create a new policy:

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

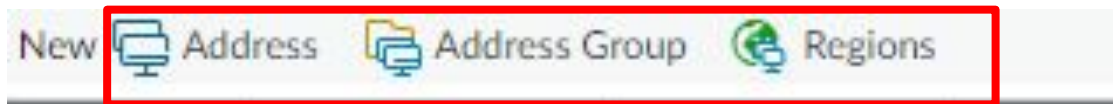
☐ Any	☐ Any	any	any
☐ SOURCE ZONE ^	☐ SOURCE ADDRESS ^	☐ SOURCE USER ^	☐ SOURCE DEVICE ^
☐ lan_zone	☐ All-LAN		
☐ + Add - Delete	☐ + Add - Delete	☐ + Add - Delete	☐ + Add - Delete

☐ Negate All but above

Security Policies

Address Options:

- Address
- Address Group
- External Dynamic List
- Region
 - Predefined - China (CN)
 - Custom



Security Policies

Create a new policy:

Security Policy Rule

General	Source	Destination	Application	Service/URL Category	Actions	Usage
---------	--------	--------------------	-------------	----------------------	---------	-------

select ☐ DESTINATION ZONE ^ ☐ wan_zone	☒ Any ☐ DESTINATION ADDRESS ^	any ☐ DESTINATION DEVICE ^
☒ Add ☐ Delete	☒ Add ☐ Delete	☒ Add ☐ Delete

☐ Negate

Security Policies

Create a new policy:

Security Policy Rule

General | Source | Destination | **Application** | Service/URL Category | Actions | Usage

☐ Any		☐ DEPENDS ON ^
☐ APPLICATIONS ^		
☐ paloalto-logging-service		
☐ paloalto-shared-services		
☐ ssl		

If the added application has a dependency, it will show here

Security Policies

Create a new policy:

Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

application-default
any
select

select

☐ SERVICE ^

☐ CDL-Ports

☒ Any

☐ URL CATEGORY ^

Security Policies

Create a new policy:

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action

Allow

▼

☐ Send ICMP Unreachable

Profile Setting

Profile Type

Group

▼

Group Profile

Outbound

▼

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding

default

Other Settings

Schedule

None

QoS Marking

None

☐ Disable Server Response Inspection

Security Policies

Create a new policy: Profile Settings

Profile Setting

Profile Type **None**

- Profiles
- Group
- None**

Profile Setting

Profile Type **Group**

Group Profile **Outbound**

Profile Setting

Profile Type Profiles

Antivirus default

Vulnerability Protection default

Anti-Spyware default

URL Filtering Custom-URL-Profile

File Blocking strict file blocking

Data Filtering None

WildFire Analysis default

Security Policies

Policies: Using Tags

Security Policy Rule

General

Source

Destination

Application

Name

LAN-to-WAN-Traffic

Rule Type

universal (default)

Description

Allow traffic from LAN to WAN zone.

Tags

Outbound

5	Block-Google-QUIC	Outbound	universal	any	any
6	Block WAN to WAN ...	none	universal	wan_zone	any
7	Rule for Exam	none	universal	lan_zone	10.0.40.103
8	Allow Traffic to CDL	Outbound	universal	lan_zone	Data
9	Email_Rule	Outbound	universal	lan_zone	All-LAN
10	LAN-to-WAN-Traffic	Outbound	universal	lan_zone	All-LAN
11	Internal_Traffic	Internal	universal	lan_zone	All-LAN

Security Policies

Policies: Grouping

Security Policy Rule

General | Source | Destination | Application

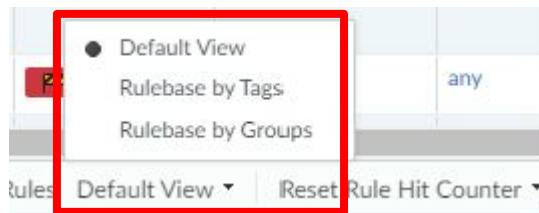
Name: LAN-to-WAN-Traffic

Rule Type: universal (default)

Description: Allow traffic from LAN to WAN zone.

Tags: Outbound

Group Rules By Tag: Outbound



Policy Optimizer

Tag Browser

7 items

TAG(RULE COUNT)	RULE NUMBER
Inbound (1)	1
Outbound (1)	2
Inbound (1)	3
Outbound (2)	4-5
none (2)	6-7
Outbound (3)	8-10
Internal (1)	11

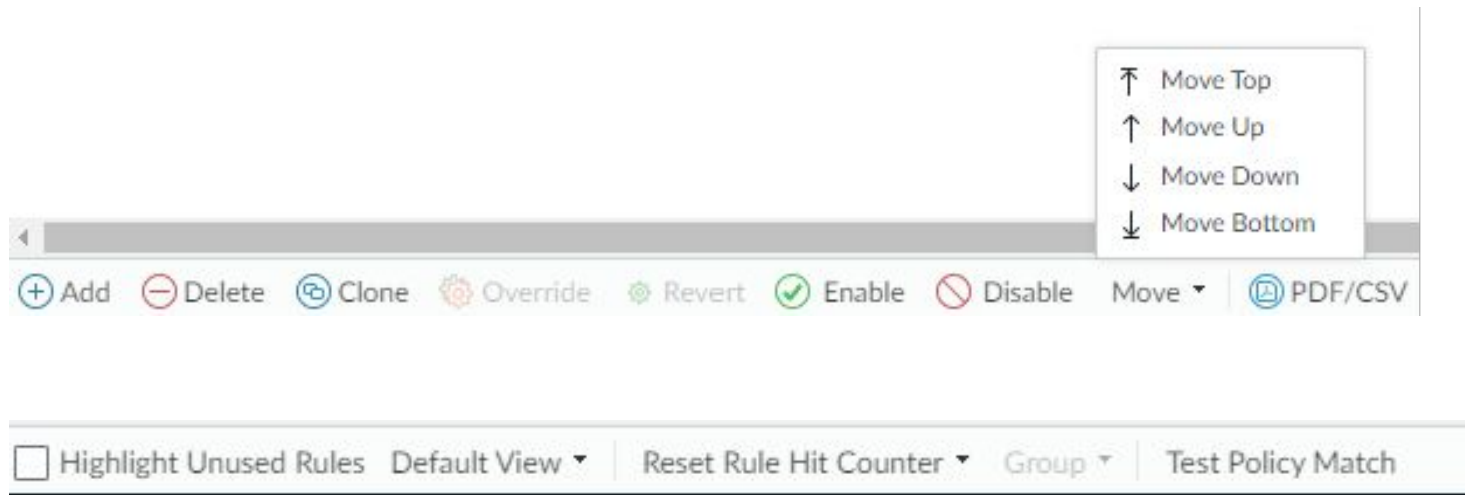
☒ Filter by first tag in rule

☒ Rule Order ☐ Alphabetical

Object: Tags

Security Policies

Policy Options:



Security Policies

Recommended Block Rules:

	NAME	TAGS	TYPE	Source				Destination	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	Geo-Block-Inbound	Inbound	universal	any	 CN  IR  KP  RU	any	any	any	any
2	Geo-Block-Outbound	Outbound	universal	any	any	any	any	any	 CN  IR  KP  RU
3	Known-Bad-EDL-Inb...	Inbound	universal	any	 Palo Alto Networks - Bulletproo...  Palo Alto Networks - High risk I...  Palo Alto Networks - Known ma...  Palo Alto Networks - Tor exit IP ...	any	any	any	any
4	Known-Bad-EDL-Ou...	Outbound	universal	any	any	any	any	any	 Palo Alto Networks - Bulletproof IP a...  Palo Alto Networks - High risk IP ad...  Palo Alto Networks - Known malicio...  Palo Alto Networks - Tor exit IP addr...

Security Policies

Recommended Block Rules:

5	Block-Google-QUIC	Outbound	universal	any	any	any	any	any	any	quic	application-...
---	-------------------	----------	-----------	-----	-----	-----	-----	-----	-----	------	-----------------

Security Policy Rule

General | Source | Destination | **Application**

☐	Any
☐	APPLICATIONS ^
☐	quic

Security Policies

Rule Usage:

Rule Usage				DAYS WITH NO NEW APPS	MODIFIED	CREATED
HIT COUNT	LAST HIT	FIRST HIT	APPS SEEN			
0	-	-	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
113247	2024-02-29 16:26:05	2024-01-05 16:18:21	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
485033	2024-02-29 16:30:53	2024-01-05 18:43:23	-	-	2024-01-05 18:39:30	2024-01-05 18:39:30
949	2024-01-12 17:26:44	2024-01-12 13:52:04	14	48	2024-01-12 17:33:16	2024-01-12 13:51:57
68955	2024-02-29 16:23:03	2024-01-05 17:21:39	3	55	2024-01-05 19:21:39	2024-01-05 17:15:37
19262	2024-02-29 16:18:16	2024-01-05 16:21:03	1	55	2024-01-05 19:21:39	2024-01-04 09:40:36
22519660	2024-02-29 16:31:00	2024-01-05 16:18:30	147	1	2024-01-05 19:21:39	2024-01-04 09:40:36
4019852	2024-02-29 16:31:01	2024-01-05 16:18:29	15	7	2024-01-05 19:21:39	2024-01-04 09:40:36

Security Policies

Applications Seen:

Applications & Usage - LAN-to-WAN-Traffic

Timeframe Anytime

Apps on Rule

☒ Any

☐ APPLICATIONS ^

Apps Seen 147

147 items → ×

☐	APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS) ▾
☒	ssl	encrypted-tunnel	4	2024-01-05	2024-02-29	604.3G
☐	paloalto-updates	software-update	2	2024-01-05	2024-02-29	347.7G
☐	hulu-base	photo-video	2	2024-01-05	2024-02-28	288.2G
☐	ipsec-esp-udp	encrypted-tunnel	2	2024-01-15	2024-02-29	29.6G
☐	facebook-base	social-networking	4	2024-01-05	2024-02-29	18.4G
☐	youtube-base	photo-video	4	2024-01-05	2024-02-29	15.4G
☐	google-base	internet-utility	4	2024-01-05	2024-02-29	14.5G

←

→

🔍 Browse

⊕ Add

⊖ Delete

🔗 Create Cloned Rule ▾

⊕ Add to This Rule

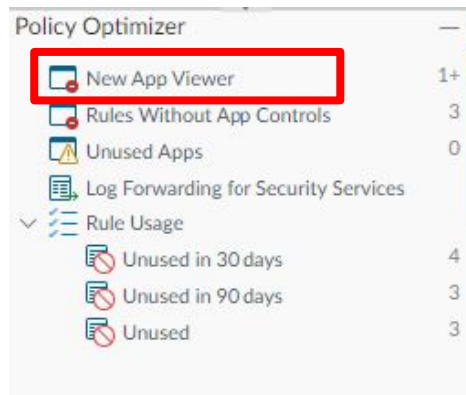
⊕ Add to Existing Rule ▾

↔ Match Usage

The last new app was discovered 1 days ago.

Security Policies

Policy Optimizer:



	NAME	SERVICE	APPLICATION	TRAFFIC (BYTES, 30 DAYS) ▼	App Usage			
					APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE
10	LAN-to-WAN-Traffic	application-...	any	1.4T	any	147	1	Compare
11	Internal_Traffic	application-...	any	1.5G	any	15	7	Compare
7	Rule for Exam	any	any	0	any	14	48	Compare

Security Policies

Policy Optimizer:

Policy Optimizer

- New App Viewer 1+
- Rules Without App Controls 3
- Unused Apps 0
- Log Forwarding for Security Services
- Rule Usage
 - Unused in 30 days 4
 - Unused in 90 days 3
 - Unused 3

Timeframe		Usage		☐ Exclude rules reset during the last 90 days			
All time		Unused					
		Rule Usage				MODIFIED	CREATED
NAME		HIT COUNT	LAST HIT	FIRST HIT	RESET DATE		
4	Known-Bad-EDL-Outbound	0	-	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
12	intrazone-default	0	-	-	-	2024-01-01 10:14:24	2024-01-01 10:14:24
13	interzone-default	0	-	-	-	2024-01-01 10:14:24	2024-01-01 10:14:24

Routing

Routing

Disclaimer:

In this section we will cover the basic configuration of routing for a Palo Alto NGFW firewall. This is a basic configuration class and NOT A ROUTING CLASS! Prior knowledge of basic routing is expected and will be assumed during this section. Configuration of dynamic routing requires matching configurations on both ends of a peering and is outside the scope of this class.

Routing

 PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

 Interfaces

 Zones

 VLANs

 Virtual Wires

 Virtual Routers

 IPSec Tunnels

 GRE Tunnels

☐

NAME

INTERFACES

CONFIGURATION

RIP

☐

default

ethernet1/5
ethernet1/3
ethernet1/1

ECMP status: Disabled

Routing

Ways to route traffic:

- Static Routing
- Dynamic Routing
 - RIP
 - OSPF
 - OSPFv3
 - BGP
 - Redistribution
- Multicast Routing

Virtual Router - default_vRouter

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

Name default_vRouter

General | ECMP

☐ INTERFACES ^

☐ ethernet1/1

☐ ethernet1/1.400

☐ ethernet1/1.410

☐ ethernet1/1.420

☐ ethernet1/2

Routing

Static Routes:

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 IPv6

NAME	DESTINA...	INTERF...
------	------------	-----------

+ Add **- Delete** **🔄 Clone**

Virtual Router - Static Route - IPv4

Name default-route

Destination 0.0.0.0/0

Interface None

Next Hop IP Address **20.1.2.3**

Admin Distance 10 - 240

Metric 10

Route Table Unicast

BFD Profile Disable BFD

☐ Path Monitoring

IP Address
Next VR
FQDN
Discard
None

Routing

Path Monitoring:

Virtual Router - Static Route - IPv4

Name

ISP-One

Destination

0.0.0.0/0

Interface

ethernet1/2

Next Hop

IP Address

1.2.3.1

Admin Distance

10 - 240

Metric

10

Route Table

Unicast

BFD Profile

Disable BFD

☒ Path Monitoring

Failure Condition

☒ Any ☐ All

Preemptive Hold Time (min)

2

☐	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
+	Add	X	Delete			

Path Monitoring Destination

Name

Google-DNS

☒

Enable

Source IP

DHCP (Use DHCP Client Address)

Destination IP

8.8.8.8

Ping Interval(sec)

3

Ping Count

5

Routing

RIP:

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

☐ Enable ☒ Reject Default Route

BFD None

Interfaces Timers Auth Profiles Export Rules

☐	INTERFACE	ENABLE	Default Route		AUTH PROFILE
			ADVERTISE	METRIC	
☐					

Interface

Interface **ethernet1/1**

☒ Enable ☐ Advertise Default Route

Auth Profile None

Mode normal

BFD Inherit Protocol's Global BFD Profile

Routing

OSPF:

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

☐ Enable ☒ Reject Default Route

Router ID IP Address

BFD None

Areas | Auth Profiles | Export Rules | Advanced

☐	AREA ID	TYPE	RANGE
--------------------------	---------	------	-------

Virtual Router - OSPF - Area

Area ID 0.0.0.0

Type	Range	Interface	Virtual Link
Type	Normal		

Routing

BGP:

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

☐ Enable

Router ID IP Address

AS Number

BFD None

General | Advanced | Peer Group | Import | Export | Conditional Adv | Aggregate | Redis

Options

☒ Reject Default Route

☐ Install Route

☒ Aggregate MED

Default Local Preference 100

AS Format ☒ 2 Byte ☐ 4 Byte

Path Selection

☐ Always Compare MED

☒ Deterministic MED comparison

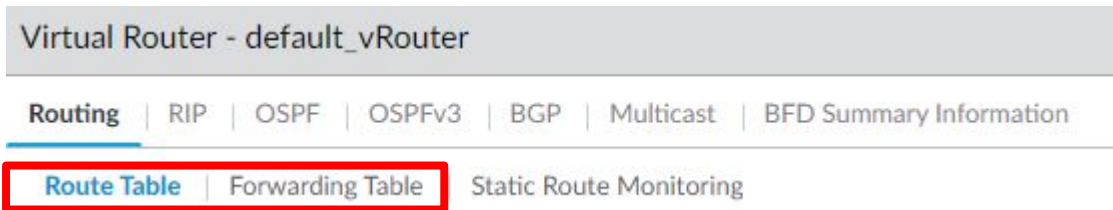
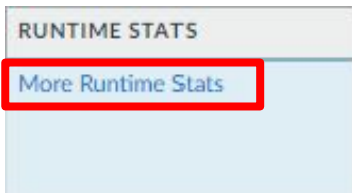
AUTH PROFILES

+ Add - Delete

Routing

Routing databases:

- Route Table (RIB) - Where all routes are stored
- Forwarding Table (FIB) - Where the route used to forward traffic is stored



Routing

Routing databases:

Virtual Router - default_vRouter



Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table

Forwarding Table

Static Route Monitoring

Route Table ☒ Unicast

☐ Multicast

Display Address Family IPv4 and IPv6



23 items



DESTINATION	NEXT HOP	METRIC	WEIGHT	FLAGS	AGE	INTERFACE
0.0.0.0/0	0.0.0.0	5		A S		sdwan.901
0.0.0.0/0	10.4.0.1	10		S		ethernet1/1
0.0.0.0/0	10.4.1.1	20		S		ethernet1/2
1.1.1.1/32	0.0.0.0	0		A H		
3.3.3.3/32	0.0.0.0	10		A S		sdwan.904
4.4.4.4/32	0.0.0.0	10		A S		sdwan.905

Routing

Routing databases:

Virtual Router - default_vRouter



Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table | **Forwarding Table** | Static Route Monitoring

Display Address Family IPv4 and IPv6

20 items → X

DESTINATION	NEXT HOP	FLAGS	INTERFACE	MTU
0.0.0.0/0	0.0.0.0	u	sdwan.901	1500
1.1.1.1/32	0.0.0.0	uh	loopback.901	1500
3.3.3.3/32	0.0.0.0	u	sdwan.904	1500
4.4.4.4/32	0.0.0.0	u	sdwan.905	1500

Routing

Routing databases: BGP

Virtual Router - default_vRouter							
Routing RIP OSPF OSPFv3 BGP Multicast BFD Summary Information							
Summary Peer Peer Group Local RIB RIB Out							
Q 2 items							
NAME	GROUP	LOCAL IP	PEER IP	PEER AS	PASSWORD SET	STATUS	STATUS DURATION (SECS.)
Denver-FW_00795400...	branch_007954...	1.1.1.1:34075	3.3.3.3:179	65003	no	Established	178409
Asheville-FW_00795400...	branch_007954...	1.1.1.1:45493	4.4.4.4:179	65004	no	Established	177667

Routing

Routing databases: BGP

Virtual Router - default_vRouter



Routing | RIP | OSPF | OSPFv3 | **BGP** | Multicast | BFD Summary Information

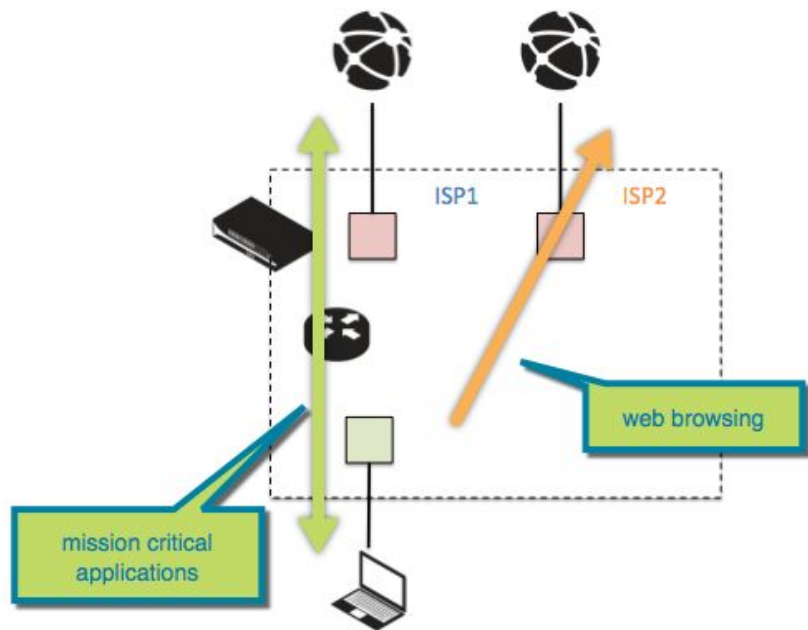
Summary | Peer | Peer Group | **Local RIB** | RIB Out

Q 3 items → ×									
PREFIX	FLAG	NEXT HOP	PEER	WEIGHT	LOCAL PREF.	AS PATH	ORIGIN	MED	FLAP COUNT
172.16.34.0/24	*	3.3.3.3	Denver-FW_0079...	0	100	65003	N/A	0	0
172.16.36.0/24	*	4.4.4.4	Asheville-FW_0079...	0	100	65004	N/A	0	0
172.16.32.0/24	*		Local	0	100		N/A	0	0

Policy Based Forwarding

Policy Based Forwarding

Policy Based Routing: [KB Link](#)



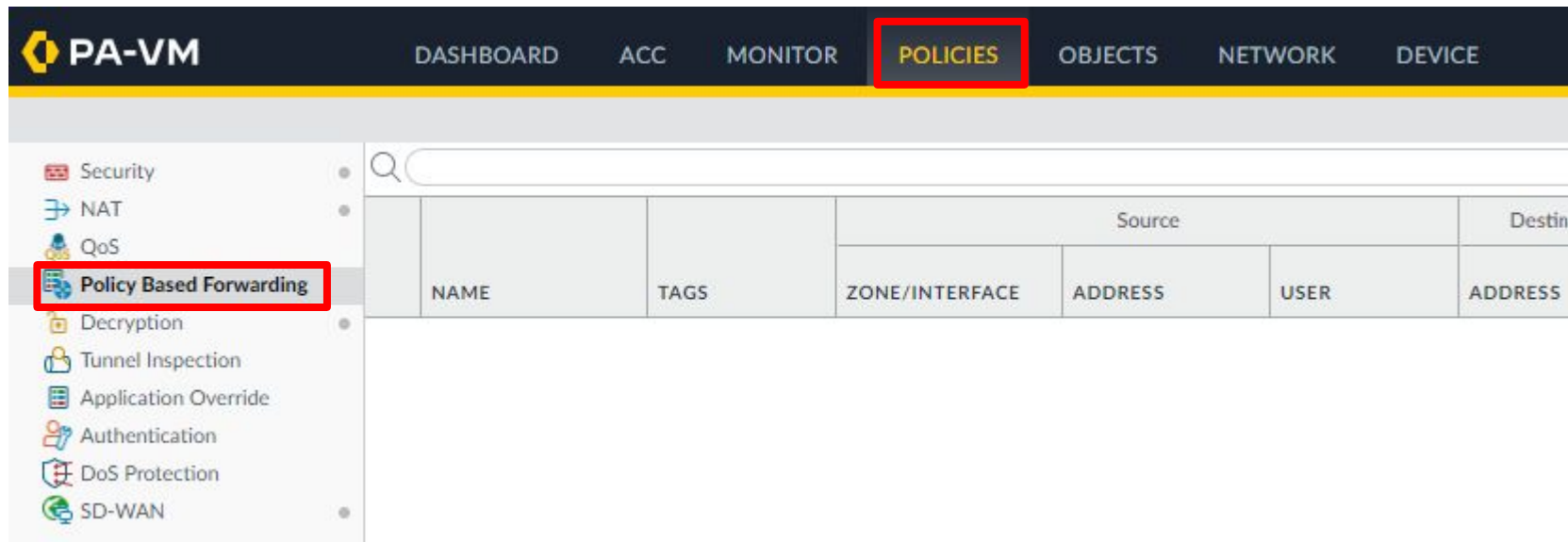
Policy Based Forwarding

Policy Based Routing: [KB Link](#)

- Create Static Routes to each ISP and set the metric of the primary lower than the secondary
- Create a Policy Based Forwarding Policy
- Create Security Policy
- Create NAT Policies

Policy Based Forwarding

Policy Based Routing: [KB Link](#)



The screenshot displays the Palo Alto Networks PA-VM management interface. The top navigation bar includes the PA-VM logo and several tabs: DASHBOARD, ACC, MONITOR, POLICIES (highlighted with a red box), OBJECTS, NETWORK, and DEVICE. On the left sidebar, a list of configuration categories is shown, with 'Policy Based Forwarding' (highlighted with a red box) selected. The main content area features a search bar and a table with the following structure:

	NAME	TAGS	Source			Destin
			ZONE/INTERFACE	ADDRESS	USER	ADDRESS

Policy Based Forwarding

Policy Based Routing: [KB Link](#)

Policy Based Forwarding Rule

General

Source

Destination/Application/Service

Forwarding

Name

ISP-PBF

Description

Tags

Group Rules By Tag

None

Audit Comment

[Audit Comment Archive](#)

Policy Based Forwarding

Policy Based Routing: [KB Link](#)

Policy Based Forwarding Rule

General **Source** Destination/Application/Service Forwarding

Type

☐ ZONE ^	☒ Any	☐ SOURCE ADDRESS ^	☐ SOURCE USER ^
☒ inside			

☐ Negate

Zone
Zone
Interface

Policy Based Forwarding

Policy Based Routing: [KB Link](#)

Policy Based Forwarding Rule



General

| Source

Destination/Application/Service

Forwarding

☒ Any	☒ Any	any
☐ DESTINATION ADDRESS ^	☐ APPLICATIONS ^	☐ SERVICE ^
+ Add - Delete	+ Add - Delete	+ Add - Delete

☐ Negate

Policy Based Forwarding

Policy Based Routing: [KB Link](#)

Policy Based Forwarding Rule

General | Source | Destination/Application/Service | **Forwarding**

Action	Forward
Egress Interface	ethernet1/1
Next Hop	IP Address
	1.2.3.4

☒ Monitor

Profile ▼

☐ Disable this rule if nexthop/monitor ip is unreachable

IP Address ▼

default
sdwan-default
Tunnel-1_Monitor
New Monitor Profile

IP Address to monitor

USER-ID

USER-ID

USER-ID Concepts:

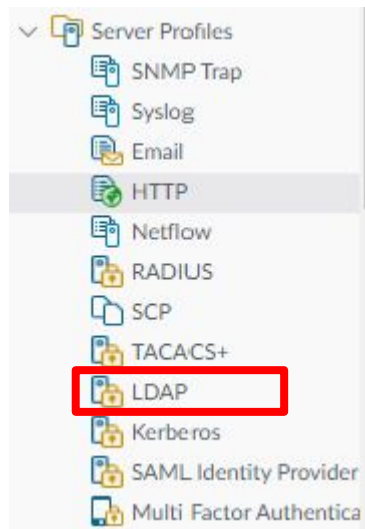
- Group Mapping - User to Group
- User Mapping - User to IP

The screenshot displays the Palo Alto Networks User-ID Agent Setup configuration page. The top navigation bar includes the PA-440 logo and tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is highlighted with a red box. On the left sidebar, the User Identification menu item is highlighted with a red box. The main content area shows the User Mapping tab selected, with other tabs like Connection Security, Terminal Server Agents, Group Mapping Settings, and Trusted Source Address visible. The Group Mapping Settings tab is also highlighted with a red box. The configuration settings for the Palo Alto Networks User-ID Agent Setup are listed below:

Setting	Value
Domain's DNS Name	
Kerberos Server Profile	
Enable Security Log	☒
Server Log Monitor Frequency (sec)	2
Enable Session	☐
Server Session Read Frequency (sec)	10
Novell eDirectory Query Interval (sec)	30

USER-ID

Server Profile:



LDAP Server Profile

Profile Name **Corp-LDAP-Profile**

☐ Administrator Use Only

Server List

NAME	LDAP SERVER	PORT
Corp-DC	10.10.10.25	389

+ Add **- Delete**

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

Base DN: **dc=netadminlab,dc-us**

Bind DN: svc_paloalto@netadminlab.us

Password:

Confirm Password:

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

☒ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

Notice: Formatting

USER-ID

Group Mapping:

Group Mapping

Name

Corp-Group-Map

Server Profile

User and Group Attributes

Group Include List

Custom Group

Server Profile

Lab-DC01

Update Interval

[60 - 86400]

Domain Setting

User Domain

Group Objects

Search Filter

Object Class

group

User Objects

Search Filter

Object Class

person

☒ Enabled

☐ Fetch list of managed devices

Group Mapping

Name

Corp-Group-Map

Server Profile

User and Group Attributes

G

User Attributes

NAME	DIRECTORY ATTRIBUTE
Primary Username	sAMAccountName
E-Mail	mail
Alternate Username 1	userPrincipalName
Alternate Username 2	
Alternate Username 3	

Group Attributes

NAME	DIRECTORY ATTRIBUTE
Group Name	name
Group Member	member
E-Mail	mail

USER-ID

Group Mapping:

Group Mapping

Name

Corp-Group-Map

Server Profile

User and Group Attributes

Group Include List

Custom Group

Available Groups

>

cn=keys

>

cn=managed service accounts

>

cn=program data

>

cn=system

▼

cn=users

cn=accounting

cn=allowed rodc password replication

cn=cert publishers

cn=cloneable domain controllers

Included Groups

netadminlab\accounting

netadminlab\engineering

USER-ID

User Mapping: PAN-OS Integrated Agent ([Document](#))

User Mapping

Connection Security

Terminal Server Agents

Group Mapping Settings

Trusted Source Address

Auth

Palo Alto Networks User-ID Agent Setup

Domain's DNS Name

Kerberos Server Profile

Enable Security Log ☒

Server Log Monitor Frequency (sec) 2

Enable Session ☐

Server Session Read Frequency (sec) 10

Novell eDirectory Query Interval (sec) 30

Syslog Service Profile

Enable Probing ☐

Probe Interval (min) 20

Enable User Identification Timeout ☒

User Identification Timeout (min) 45

Allow matching usernames without domains ☐

Server Monitoring

	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
+ Add	Delete Discover				

User Identification Monitored Server

Name	Corp-DC
Description	
☒ Enabled	
Type	Microsoft Active Directory
Transport Protocol	WMI
Network Address	10.10.10.25

USER-ID

User Mapping: PAN-OS Integrated Agent

User Mapping

Connection Security

Terminal Server Agents

Group Mapping Settings

Trusted Source Address

Auth

Palo Alto Networks User-ID Agent Setup



Domain's DNS Name

Kerberos Server Profile

Enable Security Log ☒

Server Log Monitor Frequency (sec) 2

Enable Session ☐

Server Session Read Frequency (sec) 10

Novell eDirectory Query Interval (sec) 30

Syslog Service Profile

Enable Probing ☐

Probe Interval (min) 20

Enable User Identification Timeout ☒

User Identification Timeout (min) 45

Allow matching usernames without domains ☐

Server Monitoring

☐	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
--------------------------	------	---------	------	-----------------	--------

Add Delete Discover

USER-ID

User Mapping: PAN-OS Integrated Agent

Palo Alto Networks User-ID Agent Setup - hub-stack

Server Monitor Account

Server Monitor

Client Probing

Cache

Syslog Filters

Ignore User List

Username netadminlab\svc_paloalto

Domain's DNS Name 172.16.32.25

Password

Confirm Password

Kerberos Server Profile None

Notice: Formating

USER-ID

User Mapping: Windows Agent ([Document](#))

- Install Windows Based User Agent ([Document](#))
 - Install on a domain server
- Configure Windows Based Agent ([Document](#))

User Mapping: Terminal Server Users

- Map individual users coming from a TS environment
- Supported TS
 - Windows
 - Citrix

Troubleshooting

Troubleshooting

Configuration Vs Break fix issues: [Support Datasheet](#)

- Palo Alto Support is a break fix organization.
- Palo Alto Partners are used for configuration support.

- New configurations not working are not break fix issues. Putting in a ticket for these types of issues will not get you a resolution.
- Break fix is based on previously functioning configuration or device that has stopped working. This could be due to a software upgrade, content update, bug, device failure, etc.

Troubleshooting

Management: License and Content/PANOS download issues

- Does the device have access to the internet?
- Is the device able to resolve DNS?
- Is the management interface the path to the internet?
- Did you activate the licenses or apply the authorization code?
- Do you own the license for the feature you are trying to use?
- Do you have support on the device?

Premium	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	24 x 7 phone support; advanced replacement hardware service

WildFire License	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	WildFire signature feed, integrated WildFire logs, WildFire API

Troubleshooting

Troubleshooting tool:

Device -> Troubleshooting

- Policy Match Tests

- Security Policy Match
- QoS Policy Match
- Authentication Policy Match
- Decryption/SSL Policy Match
- NAT Policy Match
- Policy Based Forwarding Policy Match
- DoS Policy Match

- Connectivity Tests

- Routing
- Ping
- Trace Route
- Log Collector Connectivity
- External Dynamic List
- Test Cloud Logging Service Status
- Test Cloud GP Service Status
- Test Wildfire
- Threat Vault
- Update Server

Troubleshooting

Ping:

Test Configuration

Select Test Ping

☐ Bypass routing tables and send directly to a host on an attached network

Count 5

☐ Don't fragment echo request packets (IPv4)

☐ Force to IPv6 destination

Interval [1 - 2]

Source

☐ Don't attempt to print addresses symbolically

Pattern

Size [0 - 65468]

Tos [1 - 255]

Ttl [1 - 255]

☐ Display detailed output

Host 8.8.8.8

Execute

Reset

Test Result

PING 8.8.8.8

Result Detail

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=11.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=11.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=11.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=11.7 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 11.286/11.527/11.790/0.218 ms

Troubleshooting

NAT Policy Match:

Test Configuration

Select Test

NAT Policy Match

From

None

To

None

Source

172.16.32.101

Destination

21.2.36.9

Source Port

[1 - 65535]

Destination Port

443

Protocol

TCP

To Interface

None

Ha Device ID

[0 - 1]

Execute

Reset

Test Result

NAT Policy Match Result

Result Detail

NAME	VALUE
Result	ISP-1-NAT-Hub

Troubleshooting

Routing Test:

Test Configuration

Select Test

Routing

☒ Fib Lookup ☐ Mfib Lookup

Destination IP

172.16.34.106

Virtual Router

default_vRouter

ECMP

Source IP

Source Port

[1 - 65535]

Destination IP

Destination Port

[1 - 65535]

Execute

Reset

Test Result

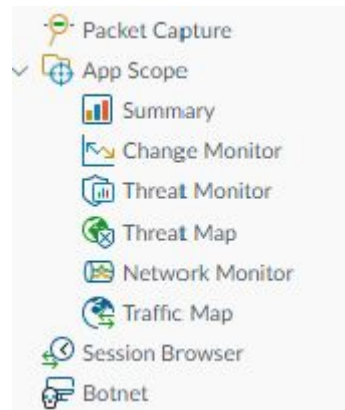
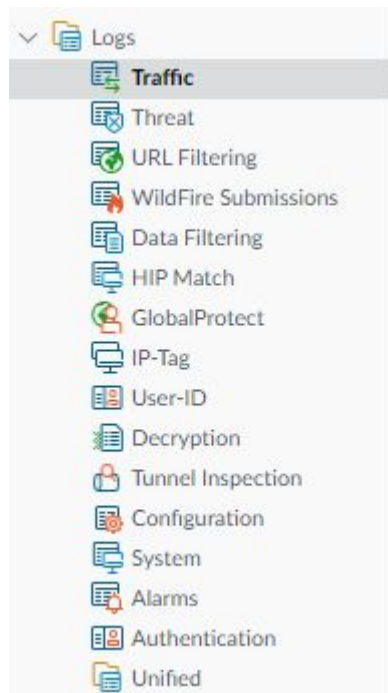
Routing Test Result

Result Detail

NAME	VALUE
Data Plane	dp0
nh	ip
Interface	sdwan.904
Metric	6543

Troubleshooting

Monitor:



Troubleshooting

Monitor: Traffic Logs

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT DEST IP	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
	03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.1.2	172.217.215.100	netadminlab\sue		172.217.215.100			443	ssl	allow	Allow-Files-MSUpdate
	03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.0.2	172.217.215.100	netadminlab\sue		172.217.215.100			443	ssl	allow	Allow-Files-MSUpdate
	03/01 09:22:53	end	inside	outside	172.16.32.25	10.4.0.2	208.67.222.222			208.67.222.222			53	dns-base	allow	Inside-to-Outside-Traffic
	03/01 09:22:53	end	inside	outside	172.16.32.25	10.4.1.2	208.67.222.222			208.67.222.222			53	dns-base	allow	Inside-to-Outside-Traffic
	03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.1.2	74.125.136.190	netadminlab\sue		74.125.136.190			443	youtube-base	allow	Inside-to-Outside-Traffic

Detailed Log View

General				Source					Destination				
Session ID 97955				Source User netadminlab\sue					Destination User				
Action allow				Source 172.16.32.101					Destination 172.217.215.100				
Action Source from-policy				Source DAG					Destination DAG				
Host ID				Country 172.16.0.0-172.31.255.255					Country United States				
Application ssl				Port 63541					Port 443				
Rule Allow-Files-MSUpdate				Zone inside					Zone outside				
Rule UUID acad8078-2f1b-425d-b92c-d89cedb437ed				Interface ethernet1/3					Interface sdwan.901				
Session End Reason tcp-fin				NAT IP 10.4.1.2					NAT IP 172.217.215.100				
				NAT Port 13375					NAT Port 443				
PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2024/03/01 09:22:53	end	ssl	allow	Allow-Files-MSUp...	acad80...	17...		any				

Troubleshooting

Changing views for information gathering.

RECEIVE TIME	TYPE	
03/01 11:15:00		Columns >
03/01 11:15:00		Adjust Columns
03/01 11:15:05	deny	☒ NAT Dest IP
03/01 11:15:05	deny	☒ Source User
03/01 11:15:00	deny	☒ Source Dynamic Address Group
03/01 11:15:00	deny	☒ Destination
03/01 11:15:00	deny	☒ Destination Dynamic Address Group
03/01 11:15:00	deny	☒ Dynamic User Group
03/01 11:15:00	deny	☒ To Port
03/01 11:15:00	deny	☒ Application
03/01 11:15:00	deny	☒ Action
03/01 11:15:00	deny	☒ Rule
03/01 11:15:00	deny	☒ Session End Reason

Troubleshooting

Filtering Logs:

				Manual ↻ ?					
				→ × + 📄 📄 ⌵					
		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT DEST IP	SOURCE USER
		03/01 11:15:05	deny	zone-to-branch	inside	172.16.34.1			netadminlab\svc...
		03/01 11:15:05	deny	zone-to-branch	inside	172.16.36.1			netadminlab\svc...
		03/01 11:15:05	deny	zone-to-branch	inside	172.16.34.1			netadminlab\svc...

Click to add
as a filter

Troubleshooting

Monitor: Traffic Log: NAT Translations

FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT SOURCE PORT	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION
lan_zone	wan_zone	192.168.18.100	173.235.189.251	0			134.238.183.164
lan_zone	wan_zone	10.0.41.102	173.235.189.251	6890			17.253.7.141
lan_zone	wan_zone	192.168.18.100	173.235.189.251	7598			170.114.52.2
lan_zone	wan_zone	192.168.18.100	173.235.189.251	14309			17.253.97.203
lan_zone	wan_zone	10.0.40.106	173.235.189.251	52330			71.18.43.229
lan_zone	lan_zone	192.168.18.100		0			192.168.18.1
lan_zone	wan_zone	10.0.40.109	173.235.189.251	28849			8.8.8.8
wan_zone	wan_zone	65.49.20.73		0			173.235.189.251

Troubleshooting

Monitor: Threat Logs

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY
	12/20 15:14:54	spyware	Parked:pixel.network.me	inside	outside	172.16.32.25			208.67.222.222			53	dns-base	alert	informational
	04/28 13:38:30	flood	PBP Packet Drop	outside		10.6.0.2			0.0.0.0			0	not-applicable	drop	high
	04/27 10:43:23	flood	PBP Packet Drop	outside		10.4.0.2			10.5.1.2			27407	not-applicable	drop	high
	04/27 10:42:19	flood	PBP Packet Drop	outside		10.4.1.2			10.5.0.2			17876	not-applicable	drop	high

Troubleshooting

Monitor: URL Logs

	RECEIVE TIME✓	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS INSERTED	HTTP/2 CONNECTION SESSION ID
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:25:29	streaming-media	streaming-media,low-risk	www.youtube.c...	inside	outside	172.16.32.101	netadminlab\sue		142.250.105.91			youtube-base	alert		98632
	03/01 09:24:58	web-advertisements	web-advertisements,low-risk	match.adsrvr.org...	inside	outside	172.16.32.101	netadminlab\sue		3.33.220.150			web-browsing	alert		98716

Troubleshooting

Monitor: Configuration

RECEIVE TIME	ADMINISTRAT...	HOST	CLIENT	COMMA...	RESULT	CONFIGURATION PATH	FULL PATH	BEFORE CHANGE	AFTER CHANGE	SEQUENCE NUMBER
02/29 14:01:08	admin	192.168.18.100	Web	commit	Submitted					7333601583554363397
02/29 14:01:02	admin	192.168.18.100	Web	delete	Succeed...	vsys vsys1 external-list CINS Army Feed	/config/devices/... list/entry[@nam... Army Feed']			7333601583554363396
02/29 14:00:43	admin	192.168.18.100	Web	delete	Succeed...	vsys vsys1 rulebase security rules Test EDL	/config/devices/... EDL']	43decde9-12f9-412c-ab9f-32019a4f27a4		7333601583554363395
02/29 13:55:53	admin	192.168.18.100	Web	commit	Submitted					7333601583554363394
02/29 13:55:44	admin	192.168.18.100	Web	set	Succeed...	vsys vsys1 rulebase security rules Test EDL	/config/devices/... EDL']		Test EDL 43decde9-12f9-412c-ab9f-32019a4f27a4 { profile-setting	7333601583554363393
02/29 13:54:09	admin	192.168.18.100	Web	set	Succeed...	vsys vsys1 external-list CINS Army Feed	/config/devices/... list/entry[@nam... Army Feed']		external-list { CINS Army Feed { type { ip { recurring { five-m	7333601583554363392
01/05 16:57:23	Panorama-admin	0.0.0.0	Panorama	commit-all	Submitted					7320737447833239553

Troubleshooting

Monitor: Unified

	LOG TYPE	RECEIVE TIME	LOG SUBTYPE	SESSION ID	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DEST... PORT	DESTINATION DYNAMIC ADDRESS GROUP	APPLICATION	ACTION	RULE	BYTES	THREAT ID/NAME	SEVERITY
	url	03/01 09:32:49	url	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	alert	Allow-Files-MSUpdate			Informational
	decryption	03/01 09:32:44	0	98962	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate			
	decryption	03/01 09:32:44	0	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate			
	decryption	03/01 09:32:44	0	98953	inside	outside	172.16.32.25			52.167.17.97	443		incomplete	allow	Allow-Files-MSUpdate			
	traffic	03/01 09:32:44	deny	98962	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate	304		
	traffic	03/01 09:32:44	deny	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate	5.2k		



LOG TYPE
url
decryption
decryption
decryption
traffic
traffic

Multiple logs consolidated into one location

Troubleshooting

Device -> Packet Capture

Configure Filtering

Manage Filters

Filtering ☒ ON Pre-Parse Match ☐ OFF

10/4 Filters Set

Configure Capturing

Packet Capture ☐ OFF

☐

STAGE

FILE

Packet Capture Filter

☐	ID	INGRESS INTERFACE	SOURCE	DESTINATION	SRC PORT	DEST PORT	PROTO
☒	1	ethernet1/1					

☒ + Add ☐ - Delete Set Selected Packet Capture Filter

Packet Capture Stage

Stage

File

File name should begin with a letter and can have letters, digits, '.', '_', and '-'

Packet Count

Byte Count

Settings

Clear All Settings

Troubleshooting

Monitor: Session Browser

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES
⊞	02/29 22:38:20	lan_zone	wan_zone	192.168.18.42	34.111.222.75	34904	443	6	paloalto-dlp-service	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	510634
⊞	03/01 11:12:00	lan_zone	wan_zone	10.0.40.109	8.8.8.8	44421	53	17	dns-base	LAN-to-WAN-Traffic	ethernet1/1.400	ethernet1/2	188
⊞	03/01 11:11:51	lan_zone	wan_zone	192.168.18.33	8.8.8.8	44251	53	17	dns-base	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	303
⊞	02/29 11:16:39	lan_zone	wan_zone	192.168.18.100	52.159.127.243	49424	443	6	windows-push-notifications	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	76156
⊞	03/01 11:11:45	lan_zone	wan_zone	192.168.18.30	192.0.2.2	44906	514	17	syslog	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	1363
⊞	03/01 11:12:07	lan_zone	wan_zone	192.168.18.42	35.184.126.116	33298	443	6	paloalto-device-telemetry	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	31294
⊞	03/01 11:09:52	lan_zone	wan_zone	192.168.18.13	107.178.249.217	37787	443	6	paloalto-updates	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	17960
⊞	03/01 11:03:09	lan_zone	wan_zone	192.168.18.50	34.235.175.181	37572	443	6	ssl	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	66513
⊞	03/01 11:11:49	lan_zone	wan_zone	10.0.40.106	104.84.231.148	60052	443	6	tiktok-base	LAN-to-WAN-Traffic	ethernet1/1.400	ethernet1/2	519372

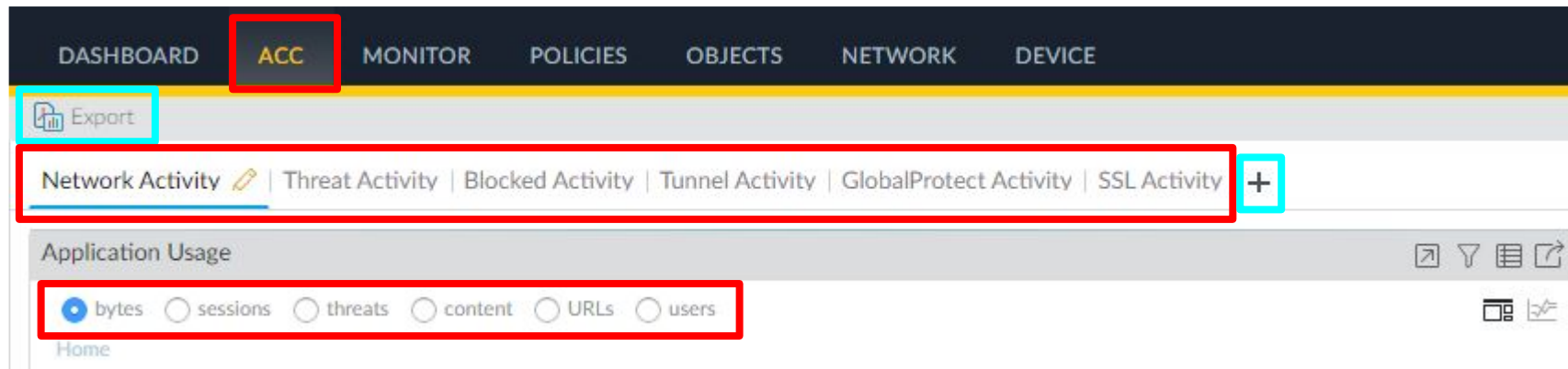
Troubleshooting

Command Line Interface: [Cheat Sheet](#)

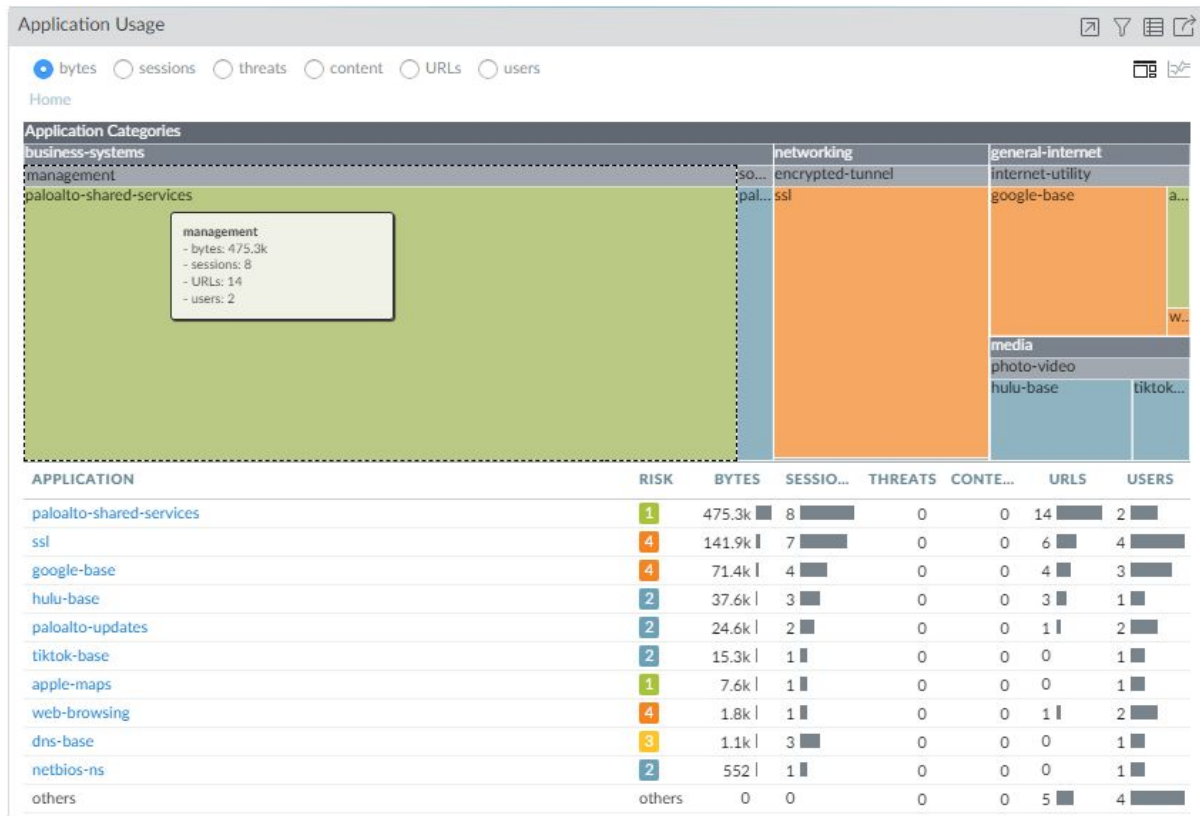
- show system info
- show system resources
- show running resource-monitor
- request restart system
- show user group-mapping statistics
- show user group-mapping state all
- show user group list
- show user group name <group-name>
- show user ip-user-mapping all
- show routing route
- ping host <destination-ip-address>
- ping source <ip-address-on-dataplane> host <destination-ip-address>

Troubleshooting

Application Control Center (ACC):



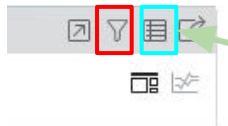
Troubleshooting



Troubleshooting

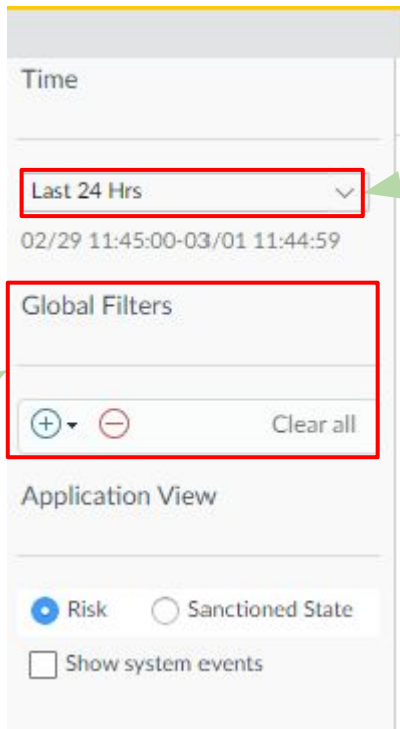
ACC: Filtering

Local Filter



Jump to logs

Global Filter

A screenshot of the Palo Alto Networks ACC interface. The 'Time' section shows a dropdown menu with 'Last 24 Hrs' selected, highlighted by a red rectangle. Below it, the date range '02/29 11:45:00-03/01 11:44:59' is displayed. The 'Global Filters' section is also highlighted with a red rectangle; it contains a plus icon, a minus icon, and a 'Clear all' button. The 'Application View' section at the bottom has radio buttons for 'Risk' (selected) and 'Sanctioned State', and a checkbox for 'Show system events'.

Time Filter

APPLICATION

palalto-shared-services

ssl

google-base

Click to add
to Global
Filter

Troubleshooting

Creating a new dashboard in the ACC:

Network Activity | Threat Activity | Blocked Activity | Tunnel Activity | GlobalProtect Activity | SSL Activity **+**

Add Custom Tab

Add Widget Group

Add Widget

Tab Name

New Dashboard

WORKSPACE

WORKSPACE

2 Column

☐ Content Activity

☐ Decryption Failure Reasons

☐ Destination IP Activity

☐ Destination Regions

☐ Destination Zones

☐ Device Profile Activity

☐ Egress Interfaces

☐ Explicit Proxy Authentication Activity

☐ Explicit Proxy Split based on Auth

☐ GlobalProtect Deployment Activity

☐ GlobalProtect Quarantine Activity

☐ HIP Information

☐ Hosts Generating Cloud Detected C2 traffic

☐ Hosts Resolving Malicious Domains

☐ Hosts Visiting Inline Categorized Malicious URLs

Resources

Resources

- [PANOS Administrator Guide](#)
- [CLI Cheat Sheet](#)
- [PANOS Recommended Releases](#)
- [Security Advisories](#)
- [Applipedia](#)
- [Hardware EoL List](#)
- [Software EoL List](#)
- [Compatibility Matrix](#)
- [SCM Pro vs Essentials](#)
- [Quick Starts and Hardware Reference](#)
- [Product Selector \(Specifications\)](#)
- [PA Series Hardware Architectures](#)

Resources

Purchasing Lab Equipment:

- Palo Alto sells equipment and software designated for testing/lab purposes. This equipment is less expensive than normal equipment with the same functionality. It is not for production as it has a different level of support.
- All customers should have a lab or mock setup for testing purposes. New configurations and software updates should never be introduced into production.
- This is a perfect way to learn and train on platforms without disruptions to your production environment.

Note: for Palo Alto Partners, this equipment is called NFR and not Lab.

Resources

Strata Logging Service (SLS)

Storing firewall logs in SLS provides AI/ML driven analytics to be used in AIOps vs only telemetry data to provide insights into your device health and security posture.

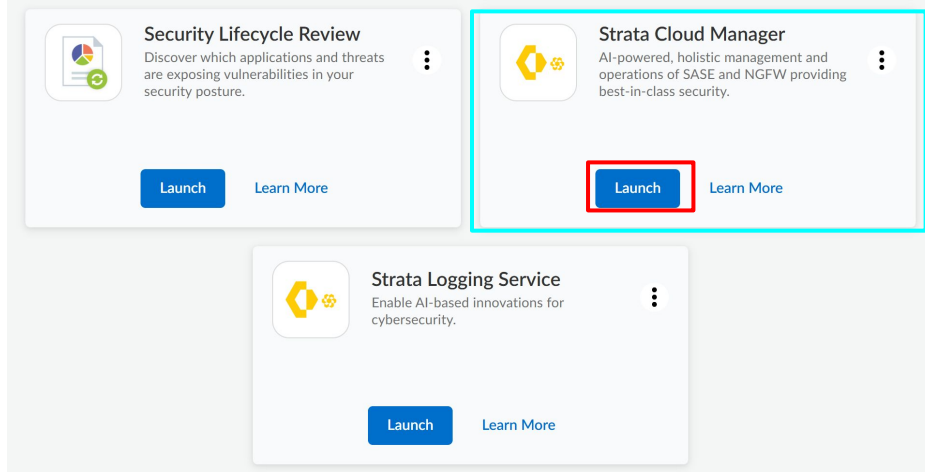
Storing firewall logs in SLS gives you an offsite repository of logs that can be accessed anywhere from the SLS Web App or Panorama.

Off site log storage allows multiple dispersed sites to log to a cloud instance instead of a single Panorama server at one location or multiple log collectors throughout the environment.

Resources

SCM:

- Install a device certificate.
- Setup SLS or Telemetry on NGFW and/or Panorama
- Send information to CDL or Telemetry
- ***** Allow 24 hours between these steps *****
- Activate your AIOps subscription in [The Hub](#)



Resources

SCM: Pro Vs Essentials

Strata Cloud Manager Essentials

Command Center and Activity Insights

Best Practices Reporting

Health Insights and Alerts

Configuration and Policy Management

Strata Logging Service - Optional Add-On
(Paid)

Strata Cloud Manager Pro

Command Center and Activity Insights

AI-Powered ADEM

Best Practices Reporting

Real-Time, Inline Best Practices

Health Insights and Alerts

AI-Powered Policy Analysis

Configuration and Policy Management

AI-Powered Operational Health
Failure Prediction, Probable Cause Analysis, Capacity Analyzer, Anomaly Detection

Strata Logging Service
Includes 1 year of retention

Software Upgrade Analysis and Recommendations

Questions?

Thank You!